



Account Reset Console

Administration Guide

Revision: May 31, 2007 – For Software Version 4.5.x

Lieberman Software Corporation - 1900 Ave of the Stars, Suite 425, Los Angeles, CA 90067

Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)

Web: www.liebsoft.com Email: support@liebsoft.com



Table of Contents

| | |
|---|----|
| Copyright Notice..... | 1 |
| License Agreement | 2 |
| Country of Origin | 3 |
| Limited Warranty | 4 |
| Pre-Usage Considerations | 5 |
| Welcome to the Account Reset Console..... | 6 |
| Thanks for using the Account Reset Console!..... | 6 |
| The Account Reset Console Web Interface..... | 6 |
| Getting Started..... | 7 |
| Configuring the Account Reset Console | 10 |
| Overview | 10 |
| Granting super-user access rights..... | 10 |
| Configuring managed domains..... | 12 |
| Setting up data sources and logging | 13 |
| Selecting program features | 14 |
| Configuring email | 17 |
| Setting up group permissions | 18 |
| Viewing logs..... | 20 |
| Configuring Verification Questions and Answers [Advanced] | 20 |
| Reviewing Data Security [Advanced]..... | 24 |
| Updating the application's appearance [Advanced]..... | 25 |
| Setting up the mobile site [Advanced] | 27 |

| | |
|---|----|
| Scheduling tasks [Advanced] | 27 |
| Configuring licensing [Advanced] | 30 |
| Changing Your Own Password..... | 31 |
| Overview | 31 |
| Changing Your Password..... | 31 |
| Resetting User Accounts | 32 |
| Overview | 32 |
| Resetting Accounts | 32 |
| Account Reset Options | 33 |
| Looking Up User Data | 33 |
| Overview | 33 |
| Resetting Accounts | 33 |
| Identity Configuration..... | 34 |
| Overview | 34 |
| Setting Up Identity Information | 35 |
| Log Viewing..... | 36 |
| Overview | 36 |
| Log Viewing Options | 36 |
| Viewing the Access Log | 37 |
| Viewing the Action Log..... | 38 |
| Scheduling Management Reports..... | 38 |
| Overview | 38 |
| Creating and Viewing Management Reports | 38 |

| | |
|---|----|
| Adding Reports | 39 |
| Running Reports Immediately | 40 |
| Editing Report Settings..... | 40 |
| Viewing Management Reports..... | 41 |
| Overview | 41 |
| Report Viewing Options..... | 42 |
| Scheduling Account Tasks | 43 |
| Overview | 43 |
| Creating and Viewing Account Tasks | 44 |
| Adding Tasks | 44 |
| Running Tasks Immediately | 45 |
| Editing Task Intervals and Actions..... | 45 |
| Viewing Account Task Reports..... | 47 |
| Overview | 47 |
| Report Viewing Options..... | 48 |
| Set Program Access Rights..... | 50 |
| Overview | 50 |
| Program Access Levels..... | 50 |
| Adding Access Rights | 51 |
| Viewing or Deleting Existing Access Rights..... | 51 |
| Set Group Access Rights | 52 |
| Overview | 52 |
| Group Access Rights..... | 52 |

| | |
|---|----|
| Adding Access Rights | 53 |
| Viewing or Deleting Existing Access Rights..... | 53 |
| Set Account Reset Features..... | 54 |
| Overview | 54 |
| Account Reset Options..... | 54 |
| Set Password Change Features..... | 56 |
| Overview | 56 |
| Password Change Options..... | 57 |
| Configuring Email Settings | 59 |
| Overview | 59 |
| Configuring Email..... | 59 |
| Appearance..... | 61 |
| Overview | 61 |
| Managing the Account Reset Console Appearance | 61 |
| Colors | 62 |
| Altering the Page Header..... | 62 |
| Customizing the Main Menu..... | 62 |
| Customizing the Side Menu | 63 |
| Customizing the Page Content..... | 63 |
| Configuring Mobile Settings..... | 64 |
| Overview | 64 |
| Managing the Mobile Settings | 64 |
| Data Sources | 65 |

| | |
|--|----|
| Overview | 65 |
| Viewing Available Data Sources..... | 65 |
| Adding a Data Source | 66 |
| Editing a Data Source | 66 |
| Editing a Microsoft Jet Data Source | 67 |
| Editing a Microsoft SQL Server Data Source | 67 |
| Editing a General ADO-Compatible Data Source | 68 |
| Logging Configuration | 68 |
| Overview | 68 |
| Viewing the Log Configuration..... | 68 |
| Changing the Log Database..... | 69 |
| Log Requirements..... | 69 |
| User Verification Configuration | 69 |
| Overview | 69 |
| Adding and Removing Questions | 70 |
| Setting the Test User..... | 71 |
| Editing Question Configurations | 71 |
| Verification Query Types | 72 |
| Designing Queries | 73 |
| Domain Configuration..... | 75 |
| Overview | 75 |
| Managing Domains | 75 |
| Viewing Domain Details | 76 |

| | |
|--|----|
| Setting the Default Domain | 76 |
| Application Security | 77 |
| Overview | 77 |
| Managing Application Security | 77 |
| Super-User Configuration | 78 |
| Overview | 78 |
| Adding new Super-User Groups..... | 78 |
| Viewing or deleting existing Super-User Groups | 79 |
| Licensing | 80 |
| Overview | 80 |
| Changing or Viewing License Information | 80 |
| The ARCWeb Site Index | 82 |
| Overview | 82 |
| Appendix A..... | 83 |
| Troubleshooting | 83 |

Copyright Notice

Copyright © 2005-2007 Lieberman Software Corporation.
All rights reserved.

The software contains proprietary information of Lieberman Software Corporation; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Lieberman Software Corporation and the client and remains the exclusive property of Lieberman Software Corporation. If you find any problems in the documentation, please report them to us in writing. Lieberman Software Corporation does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Lieberman Software Corporation.

Microsoft Windows, Window 95, Window 98, Windows NT, Windows 2000, Windows Server 2003, IIS are trademarks of the Microsoft Corporation.

License Agreement

This is a legal and binding contract between you, the end user, and Lieberman Software Corporation. By using this software, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, you should return the software and documentation as well as all accompanying items promptly for a refund.

1. Your Rights: Lieberman Software Corporation hereby grants you the right to use a single copy of this product to evaluate the product on an unlimited number of user accounts and systems for up to 30 days in a non-production environment.

When licensed by us to you for commercial use, the software can be used to manage the number of user account (passwords and settings) granted in the license. The serial number provided to you is designed for a specific named machine. If you need to move the license to another system, we will provide you with new serial numbers for those systems owned/controlled by you at no cost as long as you maintain a current support agreement with us (included for free in your first year).

Each server running our web server software requires you to purchase a separate server license as well as an appropriate number of managed user licenses. If the same user account is managed by two or more web servers, the multiple instances of the user account shall be treated as only a single user. For example, if you have three web servers managing the same domain of 4500 users, then you would need to buy three server licenses and buy 4500 user licenses.

2. Copyright. The SOFTWARE is owned by Lieberman Software Corporation and is protected by United States copyright law and international treaty provisions. Therefore, you must treat the software like any other copyrighted material (e.g. a book or musical recording) except that you may either (a) make one copy of the SOFTWARE solely for backup and archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup and archival purposes. The manual is a copyrighted work also--you may not make copies of the manual for any purpose other than the use of the software.

3. Other Restrictions: You may not rent or lease the SOFTWARE. You may not reverse engineer, de-compile, or disassemble the SOFTWARE that is provided solely as executable programs (EXE files). If the SOFTWARE is an update, any transfer must include the update and all prior versions. Some of the software provided to you is in source code form. You may not use this or any other part of this product to create derivative products for sale or use without our express written permission.

4. Notice: This software contains functionality designed to periodically notify Lieberman Software Corporation of demo usage and of the detection of suspected pirated license keys. By using this software, you consent to allow the software to send information to Lieberman Software Corporation under these circumstances, and you agree to not hold Lieberman Software Corporation responsible for the use of any or all of the information by Lieberman Software Corporation or any third party.

Country of Origin

This software was developed entirely in the United States of America.

Limited Warranty

The media (optional) and manual that make up this software are warranted by Lieberman Software Corporation to be free of defects in materials and workmanship for a period of 30-days from the date of your purchase. If you notify us within the warranty period of such defects in material and workmanship, we will replace the defective manual or media.

The sole remedy for breach of this warranty is limited to replacement of defective materials and/or refund of purchase price and does not include any other kinds of damages.

Apart from the foregoing limited warranty, the software programs are provided "AS-IS", without warranty of any kind, either expressed or implied. The entire risk as to the performance of the programs is with the purchaser. Lieberman Software Corporation does not warrant that the operation will be uninterrupted or error-free. Lieberman Software Corporation assumes no responsibility or liability of any kind for errors in the programs or documentation of/for consequences of any such errors. Lieberman Software Corporation will not be responsible for any incidental or consequential damages that result directly or indirectly from the operation of this product.

This agreement is governed by the laws of the State of California.

Should you have any questions concerning this Agreement, or if you wish to contact Lieberman Software Corporation, please write:

Lieberman Software Corporation
1900 Ave of the Stars, Suite 425
Los Angeles, CA 90067

You can also keep up to date on the latest upgrades via our website at <http://www.liebsoft.com> or email us at: sales@liebsoft.com

Pre-Usage Considerations

Please ensure that you have completed all steps in the appropriate installation checklist before you begin attempting to manage the Account Reset Console. Installation checklists can be found in the accompanying document, *ArcWeb Install Guide*.

If you have any questions or concerns about this program's installation or operation before or after it has been installed, please contact our support department for assistance. Incorrect installation or poor security practices could allow the compromise of your passwords.

When used and installed properly, this program provides excellent performance, speed and security for your password management. Call us if you have **any** questions about this product.

Welcome to the Account Reset Console

Thanks for using the Account Reset Console!

Thank you for using Lieberman Software's Account Reset Console! The Account Reset Console, or "ARCWeb" for short, provides your Help Desk with the ability to reset domain account passwords/account flags, and allows users to reset their own forgotten or expiring passwords in a fully audited and delegated manner via any web browser. Features of the Account Reset Console include:

- The ability to control which users or members of the Help Desk have access to the application
- The ability to regulate which group(s) or users each Help Desk person is allowed to manage
- The ability to reset or delegate the authority to reset disabled and locked accounts
- The ability to allow authorized users to change or reset their own passwords, eliminating Help Desk calls for password resets
- The ability to allow users to reset their own forgotten passwords based on user identity validation against any relational database
- The ability to schedule tasks and reports on all managed users
- And more!

The Account Reset Console Web Interface

The Account Reset Console is an entirely web-based application which can be completely re-skinned to match your corporate colors and logos. It can be accessed through any web browser. The Account Reset Console's user interface is designed to be simple to understand and to put all features of the tool no more than a few clicks away, for quick and easy administration. Here is a quick introduction to the interface:

The screenshot shows the 'Account Reset Console' interface. At the top, there is a header with the Lieberman Software logo (1) and the title 'Account Reset Console' (2). Below the header, a navigation bar contains links for 'Accounts' (3), 'Scheduling/Reporting' (5), 'Management', 'Configuration', and 'Index'. A 'Log Out' link (4) is located in the top right corner. The main content area is titled 'Reset User Account' and includes a sidebar with links like 'Look up User Data', 'Change My Password', and 'Set Up My Identity' (6). The main form prompts the user to 'Enter Username and a new Password (twice) for the account to be reset.' and includes fields for 'Username', 'Password', and 'Password (again)', along with several checkboxes for account options and a 'Reset Account' button.

1. Corporate Logo – your corporate logo can be put here instead of the Lieberman Software logo.
2. Tagline – your own tagline can be used here. In addition, nearly all colors in the Account Reset Console can be changed to match your own corporate identity.
3. Logged-in User: the user currently logged into the system at this web browser.
4. Logout link: Logs the user out of the system.
5. Main menu: Each link on the main menu represents a separate area of activity. Users with lower privilege levels will see only a few main menu items, such as “Accounts” (for normal users) or “Accounts” and “Scheduling/Reporting” (for Help Desk Managers).
6. Side Menu: Each main-menu section is subdivided into several “pages”, which can be accessed through the side menu.

Getting Started

Once you have completely installed the Account Reset Console, you will begin by logging into the web interface and configuring the product. You will also need to set the group privileges to allow help desk and admin personnel to utilize the appropriate parts of the application.

Begin by logging into the Account Reset Console. You will need to use an account that is a member of the initial administrator’s group you specified in the installation process. If your account is not a member of this initial group you will receive an error message explaining why you are not permitted to log in.

 **LIEBERMAN SOFTWARE**
Account Reset Console

Please log in to access the Account Reset Console.

Username

Password

Domain ▼

Forgot your password / Locked out?
Click here to:



©2005-2007 Lieberman Software Corporation
Web: 070530 (ArcWeb)
ACL: 4.50 (070530) ARC: 4.50 (070530)

Once you log into the Account Reset Console you should see a series of top-level menu options which look similar to the ones below. If you do not see all the menus, you have logged in with an account that is not a member of the initial administrative group, and the Account Reset Console is restricting your access to certain parts of the interface.

 **LIEBERMAN SOFTWARE**
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts **Scheduling/Reporting** **Management** **Configuration** **Index**

| Reset User Account | |
|---|---|
| <p>Reset User Account</p> <p>Look up User Data</p> <p>Change My Password</p> <p>Set Up My Identity</p> | <p style="text-align: center;">Enter Username and a new Password (twice) for the account to be reset.</p> <p>Username <input type="text"/></p> <p>Domain <input type="text" value="SECURUS"/> ▼</p> <p><input checked="" type="checkbox"/> Reset the account password</p> <p>Password <input type="password"/></p> <p>Password (again) <input type="password"/></p> <p><input checked="" type="checkbox"/> Enable account if disabled</p> <p><input checked="" type="checkbox"/> Unlock account if locked</p> <p><input checked="" type="checkbox"/> Force user to change password on next login</p> <p style="text-align: center;"><input type="button" value="Reset Account"/></p> |

The top-level menus represent different parts of the ARCWeb product:

Accounts Scheduling/Reporting Management Configuration Index

- **Accounts** – this menu contains the direct account manipulation pages. Ordinary users use these pages to reset their own passwords and configure their answers for identity verification. Help desk users use these pages to reset other users' accounts.
- **Scheduling/Reporting** – this menu contains pages for viewing the access and reset logs, and for scheduling tasks and viewing the reports generated by these tasks. These pages are generally for help desk managers.
- **Management** – this menu contains pages for setting group permissions, program features, and application appearance (skinning). This is also where email will be configured.
- **Configuration** – this menu contains pages for domain and data source management, verification questions, log database location, and application licensing.
- **Index** – this menu links to the index page to the entire application, allowing you to immediately jump to any page you have rights to access.

Once you have logged onto the Account Reset Console you should begin by configuring the application to fit your network and your particular needs.

Configuring the Account Reset Console

Overview

Once you have installed and logged into the Account Reset Console, there are a few steps you will need to take to configure the tool to function properly with your network. You can use the tool at any point, but properly configuring it will unlock the full functionality of the product and allow you to explore every feature it offers.

We recommend that you begin working with the Account Reset Console by:

1. Granting Super-User access rights
2. Configuring managed domains
3. Setting up data sources and logging
4. Selecting program features
5. Configuring email
6. Setting up group permissions
7. Viewing logs

Once you have finished these, the core functionality of the Account Reset Console will be completely accessible to yourself and those you delegate authority to. You can then proceed to configure the advanced features of ARCWeb:

1. Configuring verification questions and answers
2. Reviewing data security
3. Updating the application's appearance
4. Setting up the mobile site (if applicable)
5. Scheduling tasks
6. Configuring licensing

Granting super-user access rights

When you first installed Account Reset Console, you were asked for a group that would be granted initial access. This group is also granted Super-User access. Super-User access allows the users of the identified group to be able to perform any actions in the tool including changing verification questions, database settings, and licensing. You can update these permissions at any time, but if you have certain administration accounts or groups that you would like to have unfettered access to the tool, now is a good time to configure them for your convenience.

You can find super-user configuration under the "Configuration" main menu item, under the "Super-Users" side menu tab:

Manage Super-User Groups

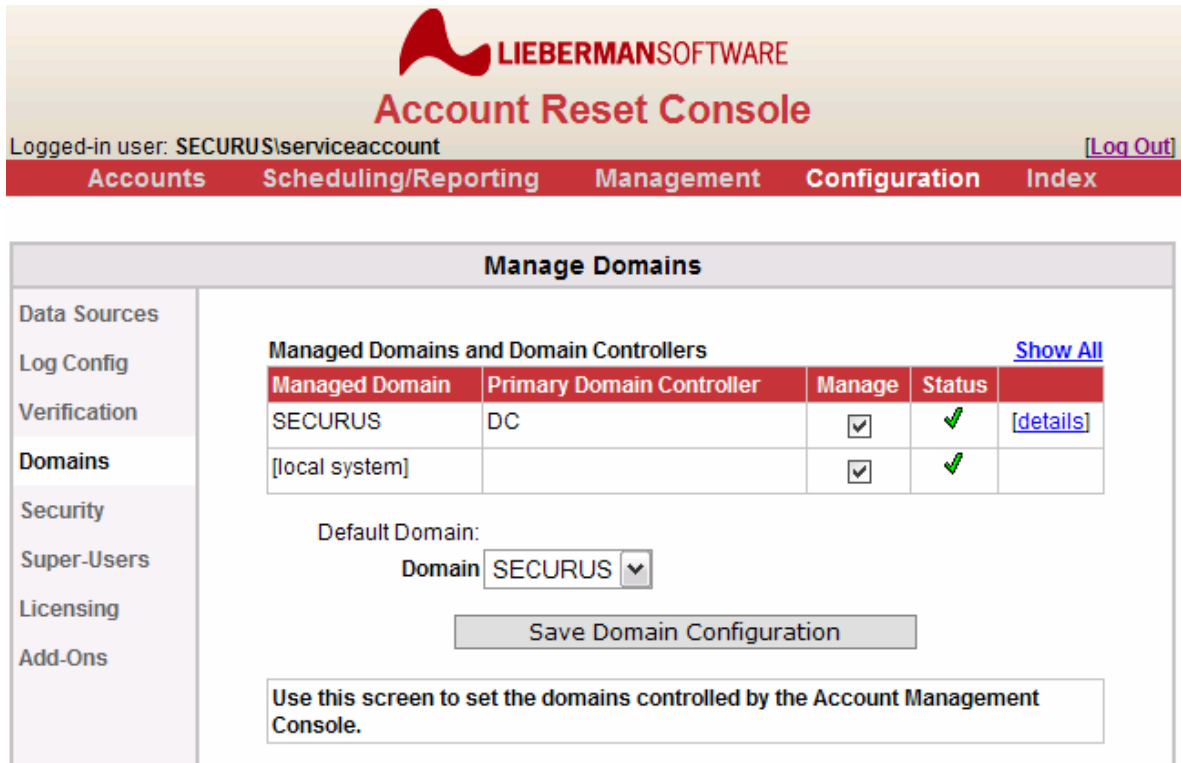
| Data Sources | <p>Add a new application superuser group:</p> <p>SECURUS <input type="text" value="Enter groupname here"/></p> <p><input type="button" value="Add SuperUsers"/></p> <p>Global Program Access Rules</p> <table border="1"><thead><tr><th>Global Access Category</th><th>Allowed Windows Groups</th></tr></thead><tbody><tr><td>Allow application config</td><td>securus\domain admins [del]</td></tr></tbody></table> <p>Use this screen to grant complete application-control access to members of Windows Groups.</p> | Global Access Category | Allowed Windows Groups | Allow application config | securus\domain admins [del] |
|--------------------------|--|---|------------------------|--------------------------|---|
| Global Access Category | | Allowed Windows Groups | | | |
| Allow application config | | securus\domain admins [del] | | | |
| Log Config | | | | | |
| Verification | | | | | |
| Domains | | | | | |
| Security | | | | | |
| Super-Users | | | | | |
| Licensing | | | | | |
| Add-Ons | | | | | |

Add your groups by entering their group name (and domain, if appropriate) into the entry fields and clicking “Add SuperUsers” for each one.

Granting super-user permissions to a group allows them to access any component of the Account Reset Console interface. For more information on super-users, see the dedicated “Super-User Configuration” section later in this document.

Configuring managed domains

Once you have entered your selected super-user groups it is time to configure the specific domains that the Account Reset Console will be able to manage. Domain configurations can be found under the “Configuration” main menu item, in the “Domains” side menu tab.



The screenshot shows the 'Account Reset Console' interface. At the top, it displays the Lieberman Software logo and the title 'Account Reset Console'. Below the title, it shows the logged-in user as 'SECURUS\serviceaccount' and a '[Log Out]' link. The main navigation bar includes 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The 'Manage Domains' section is active, showing a table of managed domains and domain controllers. The table has columns for 'Managed Domain', 'Primary Domain Controller', 'Manage', and 'Status'. Two domains are listed: 'SECURUS' and '[local system]'. Both have a checked 'Manage' box and a green checkmark in the 'Status' column. A 'Show All' link is visible to the right of the table. Below the table, there is a 'Default Domain:' label and a dropdown menu currently set to 'SECURUS'. A 'Save Domain Configuration' button is located below the dropdown. At the bottom of the interface, a warning message states: 'Use this screen to set the domains controlled by the Account Management Console.'

| Managed Domain | Primary Domain Controller | Manage | Status | |
|----------------|---------------------------|-------------------------------------|--------|---------------------------|
| SECURUS | DC | <input checked="" type="checkbox"/> | ✓ | [details] |
| [local system] | | <input checked="" type="checkbox"/> | ✓ | |

The Account Reset Console will allow you to select (enable) any domain for which your COM+ account has administrator privileges:

WARNING: The COM+ account for the ARCWeb COM+ components does not have administrator privileges on this domain. ARCWeb will not be able to make changes on this domain.

You can see any status error messages by clicking the **[details]** link for a given domain.

If you cannot enable the domain you wish to manage, you may re-run the installer and use a different account with the appropriate permissions for the COM+ portion of the application, or grant that account required permissions on the target domain. You can also choose to allow ARCWeb to manage the local by choosing the [local system] option.

For more information on domain configuration, see the section titled “Domain Configuration” later in this document.

Setting up data sources and logging

Account Reset Console 4.X requires Microsoft MSDE/SQL Express or SQL Server 2000/2005 or later for logging and user verification purposes. Lieberman Software Corporation recommends Microsoft SQL Server 2000 or 2005 as the optimal solution for these purposes.

The Account Reset Console is designed to use a variety of databases for logging and verification purposes. The “Data Sources” page is the single management point for configuring these databases. Once a database is configured here, it can be used by other parts of the system. You can find this page under the “Configuration” main menu item, in the “Data Sources” side menu tab.

Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts Scheduling/Reporting Management **Configuration** Index

Manage Data Sources

| Data Sources | | | |
|-------------------------------------|------------|---------|--|
| Add or configure data sources here: | | | |
| Name | Type | Working | Actions |
| Default Database | SQL Server | ✓ | [Edit] [del] |

New Data Source

Name:

Type:

Data Sources
Log Config
Verification
Domains
Security
Super-Users
Licensing
Add-Ons

For evaluation purposes the default installed database should suffice. If you need to configure more databases later, the section titled “Data Sources” later in this document fully documents the process of adding a new data source or editing existing data sources. For initial evaluation it should be sufficient to note that the default data source (“Default Log”) should be functional (have a green check as shown above). If you have installed the product and the data source does not have the green check, you will need to return to the installation checklist and double-check the database configuration steps.

Once you have functioning data sources, you will need to examine the logging configuration. This page is the next one down on the side menu bar, still in the “Configuration” main menu section, under the “Log Config” side menu tab. The **Status** line of the page should have a green checkmark next to it, indicating that the default database is functioning.

| Configure ARCWeb Logging | | | | | | | |
|---|---|------|------------------|------|------------|--------|--|
| <ul style="list-style-type: none"> Data Sources <li style="background-color: #d3d3d3;">Log Config Verification Domains Security Super-Users Licensing Add-Ons | <p style="text-align: center;">Select the logging database information below</p> <p style="text-align: center;">Logging Data Source: <input style="width: 100px;" type="text" value="Default Database"/> <input type="button" value="v"/></p> <p style="text-align: center;">Current Settings</p> <table style="margin-left: auto; margin-right: auto;"> <tr><td style="padding: 2px;">Name</td><td>Default Database</td></tr> <tr><td style="padding: 2px;">Type</td><td>SQL Server</td></tr> <tr><td style="padding: 2px;">Status</td><td>✔ Working</td></tr> </table> <p style="text-align: center; margin-top: 10px;"><input type="button" value="Update logging settings"/></p> | Name | Default Database | Type | SQL Server | Status | ✔ Working |
| Name | Default Database | | | | | | |
| Type | SQL Server | | | | | | |
| Status | ✔ Working | | | | | | |

You can select any data source as your log destination using the dropdown box on this page. The Account Reset Console will reject your choice if you select a non-SQL Server data source. If you select a SQL Server data source without extant tables, ARCWeb will be able to create the appropriate database tables for you. You can find information on the database table requirements and setting alternate databases in the “Logging Configuration” section later in this document.


For evaluation purposes the default database should be all you need.

Selecting program features

The core features of the Account Reset Console can be configured by administrators and super-users. They are divided into two sections: **Account Reset Features** and **Password Change Features**. Account Reset Features apply to usage of the Account Reset Console by Help Desk users who are resetting other users’ accounts. Password Change Features apply to usage of the Account Reset Console by users who are resetting their own passwords.

You can find both sets of features under the “Management” top-level menu item. On the side menu they will be items 3 and 4, “Account Reset Features” and “Password Change Features”.

Account Reset Features

**LIEBERMAN SOFTWARE**
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts Scheduling/Reporting Management Configuration Index

Manage Account Reset Features

| | |
|---|--|
| <p>Program Access</p> <p>Group Access</p> <p>Account Reset Features</p> <p>Password Change Features</p> <p>Configure Email Settings</p> <p>Appearance</p> <p>Mobile Settings</p> | <p style="border: 1px solid gray; padding: 5px;">These features are for IT personnel resetting arbitrary user accounts. Change these settings to allow the IT personnel to reset user accounts.</p> <p>Account Reset Features</p> <p><input checked="" type="checkbox"/> Reset passwords through Account Reset Console</p> <p><input checked="" type="checkbox"/> Allow Help Desk to view user identity information</p> <p>Enable disabled accounts <input type="radio"/> Always <input checked="" type="radio"/> Optional <input type="radio"/> Never</p> <p>Unlock locked accounts <input type="radio"/> Always <input checked="" type="radio"/> Optional <input type="radio"/> Never</p> <p>Require that reset passwords be changed on next login (ignored when user cannot change password) <input type="radio"/> Always <input checked="" type="radio"/> Optional <input type="radio"/> Never</p> <p><input type="checkbox"/> Display the following HTML message to Help Desk personnel resetting accounts</p> <div style="border: 1px solid gray; height: 60px; width: 100%;"></div> <p><input type="checkbox"/> Email users notifications that the Help Desk has reset their passwords</p> <div style="border: 1px solid gray; padding: 5px;"><p>Dear #RealName#,</p><p>This is an automatic notification that your account password has just been changed. You should only be receiving</p></div> <p><input checked="" type="radio"/> Plain Text <input type="radio"/> HTML Mail <input type="radio"/> Rich Text</p> <p>Email keywords: #RealName# - User's full name as stored in Active Directory. #UserName# - User's logon name. #Email# - User's email address as stored in Active Directory. #Password# - The user's new password.</p> <p style="text-align: center; margin-top: 10px;"><input type="button" value="Save Program Features"/></p> |
|---|--|

The Account Reset features allow you to configure what operations Help Desk personnel can perform on accounts they are resetting. By default, the options should allow all actions on the account. The settings on this page directly affect the available controls on the “Reset User Account” page seen by Help Desk personnel. For evaluating the product the default options should suffice. However, you may find it valuable to switch between this page and the “Reset User Account” page to see exactly what occurs as you change the settings. For more information on these features, see the “Set Account Reset Features” and “Resetting User Accounts” sections later in this document.

Password Change Features

The screenshot shows the 'Account Reset Console' interface. At the top, there is a navigation bar with the following items: 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The user is logged in as 'SECURUS\serviceaccount' and there is a '[Log Out]' link. The main content area is titled 'Manage Password Change Features'. On the left, there is a sidebar menu with options: 'Program Access', 'Group Access', 'Account Reset Features', 'Password Change Features' (which is selected), 'Configure Email Settings', 'Appearance', and 'Mobile Settings'. The main content area contains the following text and settings:

These features are for general users resetting their own passwords. Change these settings to allow users to update their own account information.

Password Change Features

- Allow users to change their own passwords using the web interface
- When users change their own passwords, emulate their user account to comply with domain policies
- When users change their own passwords, expire them so that they must be changed on next login (ignored when user cannot change password)
- Allow self service unlock and password reset through ARC (via ID verification)
- Allow self service unlock and password reset through Credential Provider / Gina (via ID verification)

Verification allowed wrong answers:

Verification wrong answers timeout(minutes):

The Password Change Features page allows you to configure the behavior of ARCWeb when users reset their own passwords. Note that the checkbox entitled “Allow lost password recovery through ARC” may be enabled but will only function properly once you have configured your verification questions and answers (in the advanced features).

The default settings should be sufficient for initial evaluation of the product. For more information on this page, see the “Set Password Change Features” section later in this document.

Configuring email

If you want the Account Reset Console to be able to notify users via email of account or password resets, or to be able to email administrators and managers of scheduled task completion or failure, you will need to configure the email system. You can find the email configuration page under the “Management” main menu item and the “Configure Email Settings” side menu tab.

The screenshot shows the 'Account Reset Console' interface. At the top, there is a logo for 'LIEBERMAN SOFTWARE' and the title 'Account Reset Console'. Below the title, it indicates the logged-in user as 'SECURUS\serviceaccount' and provides a '[Log Out]' link. A navigation bar contains the following items: 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The main content area is titled 'Configure Email Settings' and features a left-hand sidebar with a tree view of menu items: 'Program Access', 'Group Access', 'Account Reset Features', 'Password Change Features', 'Configure Email Settings' (which is highlighted), 'Appearance', and 'Mobile Settings'. The main content area contains a text box explaining that the page allows configuring email settings for ARCWeb. Below this is the 'Manage Email Server Settings' section, which includes several input fields: 'Server Name' (mail.yourco.com), a checked checkbox for 'This email server requires authentication', 'Username' (userName), 'Password' (masked with dots), 'Source Email Address' (accountresetconsole), 'Reply Email Address' (admin@yourco.com), and 'Admin Email Address' (admin@yourco.com). A 'Save Email Configuration' button is located at the bottom of the form.

You will need to use appropriate settings for your network and mail server configuration. For more information on configuring email settings, see “Configuring Email Settings” later in this document.

Setting up group permissions

The final step before you begin using the basic features of the Account Reset Console is to delegate login and account reset permissions to your chosen groups. ARCWeb uses two types of account permission, **Program Access** and **Group Access**. Program Access allows you to delegate login rights and interface level privileges to groups; Group Access allows you to delegate the authority to reset specific other users' accounts to groups. Group permissions are the first two side menu tabs under the "Management" main menu tab.

Program Access

You will need to begin by assigning different user groups appropriate web interface access permissions. This is available under "Program Access". To grant permissions to a group, select the appropriate permissions and click "Add Rule".

LIEBERMAN SOFTWARE
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts **Scheduling/Reporting** **Management** **Configuration** **Index**

Manage Program Access Permissions

Program Access
Group Access
Account Reset Features
Password Change Features
Configure Email Settings
Appearance
Mobile Settings

Add a New Global Program Access Rule:

Allow Web Logon
 Allow Reset of Other Users' Accounts
 View Console Logs and Task Reports
 Manage All Web Access Controls

Domain: SECURUS

Global Program Access Rules


| Global Access Category | Allowed Windows Groups |
|--------------------------------------|---|
| Allow Web Logon | securus\domain admins [del] |
| | SECURUS\can reset [del] |
| | SECURUS\can be reset [del] |
| Manage All Web Access Controls | securus\domain admins [del] |
| Allow Reset of Other Users' Accounts | securus\domain admins [del] |
| | SECURUS\can reset [del] |
| View Console Logs and Task Reports | securus\domain admins [del] |

- Allow Web Logon: Allows users to log onto the Account Reset Console to reset their own passwords or configure verification answers.
- Allow Reset of Other Users' Accounts: Allows users to reset other accounts **if they have been granted permissions for the specific target user in the "Group Access" page**. See the next section for more information.
- View Console Logs and Task Reports: Allows users to view the Account Reset Console's activity logs and schedule and view tasks and reports.
- Manage All Web Access Controls: Allows users to specify program features and group permissions.

For more information on how to use this page, please see "Set Program Access Rights", later in this document.

Group Access

Each group which has been granted the "Allow Reset of Other Users' Accounts" access right will have access to the "Reset User Account" page in ARCWeb. However, their requests to reset accounts will be rejected unless you also grant them the rights to reset other users' accounts. The "Group Access" page allows you to specify which target groups can be reset.


LIEBERMANSOFTWARE
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

[Accounts](#) [Scheduling/Reporting](#) [Management](#) [Configuration](#) [Index](#)

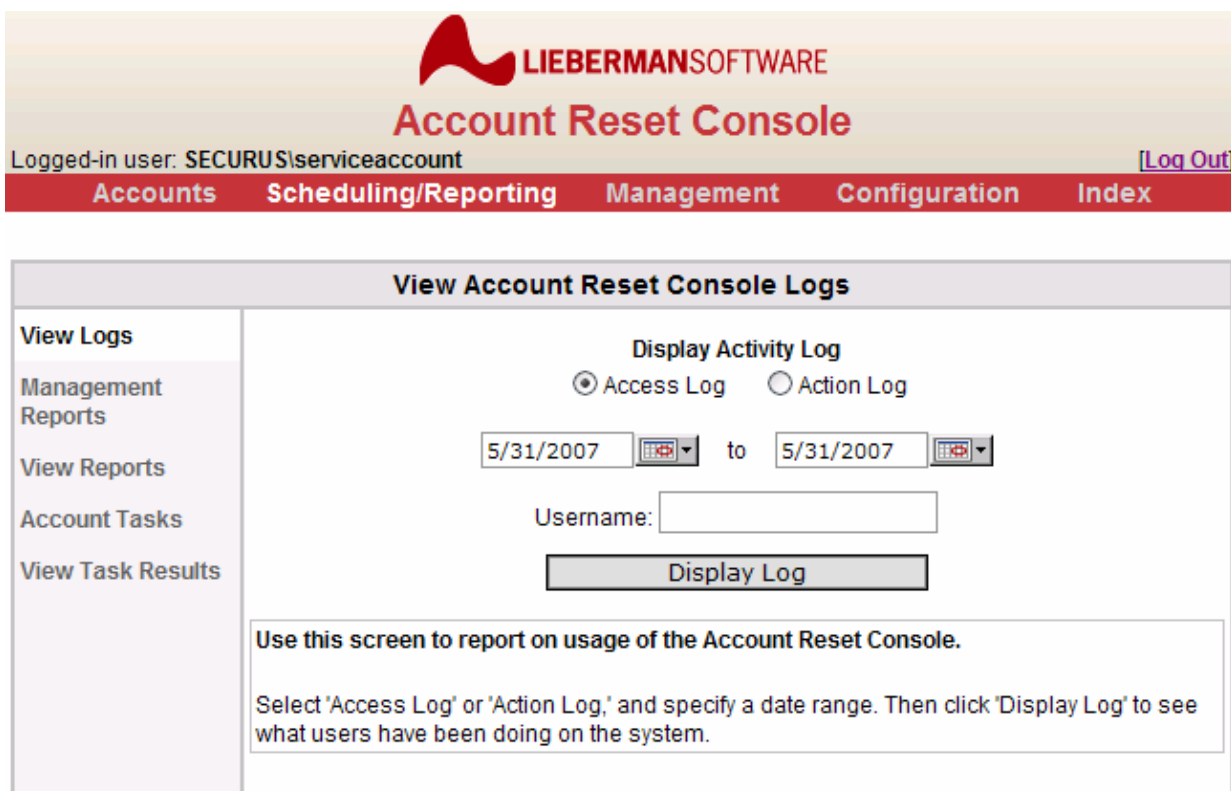
Manage Group Access Permissions

| Program Access Group Access Account Reset Features Password Change Features Configure Email Settings Appearance Mobile Settings | <p>Add a New Group Access Rule</p> <p>Administrative Group: <input type="text" value="SECURUS"/> <input type="button" value="Enter groupname here"/></p> <p>Managed Group: <input type="text" value="SECURUS"/> <input type="button" value="Enter groupname here"/></p> <p>Permissions: <input checked="" type="checkbox"/> Reset Password <input type="checkbox"/> View User Answers</p> <p style="text-align: right;"><input type="button" value="Add Group Access Rule"/></p> <p>Group Access Rules - Account Reset Privileges</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e67e22; color: white;"> <th style="width: 50%;">Administrative Group</th> <th style="width: 50%;">Managed Groups</th> </tr> </thead> <tbody> <tr> <td>SECURUS\can reset</td> <td>SECURUS\can be reset [del]</td> </tr> <tr> <td>SECURUS\domain admins</td> <td>SECURUS\domain users [del]</td> </tr> </tbody> </table> <p>Group Access Rules - View User Answers Privileges</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e67e22; color: white;"> <th style="width: 50%;">Administrative Group</th> <th style="width: 50%;">Managed Groups</th> </tr> </thead> <tbody> <tr> <td>SECURUS\can reset</td> <td>SECURUS\can be reset [del]</td> </tr> <tr> <td>SECURUS\domain admins</td> <td>SECURUS\domain users [del]</td> </tr> </tbody> </table> | Administrative Group | Managed Groups | SECURUS\can reset | SECURUS\can be reset [del] | SECURUS\domain admins | SECURUS\domain users [del] | Administrative Group | Managed Groups | SECURUS\can reset | SECURUS\can be reset [del] | SECURUS\domain admins | SECURUS\domain users [del] |
|--|---|----------------------|----------------|-------------------|--|-----------------------|--|----------------------|----------------|-------------------|--|-----------------------|--|
| Administrative Group | Managed Groups | | | | | | | | | | | | |
| SECURUS\can reset | SECURUS\can be reset [del] | | | | | | | | | | | | |
| SECURUS\domain admins | SECURUS\domain users [del] | | | | | | | | | | | | |
| Administrative Group | Managed Groups | | | | | | | | | | | | |
| SECURUS\can reset | SECURUS\can be reset [del] | | | | | | | | | | | | |
| SECURUS\domain admins | SECURUS\domain users [del] | | | | | | | | | | | | |

Only by setting BOTH the “Allow Reset of Other Users’ Accounts” program access level AND the appropriate group access rule will a help desk user be able to reset another user’s account. For more information, please see the “Set Group Access Rights” section later in this document.

Viewing logs

You can view the logs generated by the Account Reset Console in the “Scheduling/Reporting” main menu section, under the “View Logs” side menu tab.



LIEBERMAN SOFTWARE
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts **Scheduling/Reporting** **Management** **Configuration** **Index**

View Account Reset Console Logs

View Logs
Management Reports
View Reports
Account Tasks
View Task Results

Display Activity Log
 Access Log Action Log

5/31/2007 to 5/31/2007

Username:

Display Log

Use this screen to report on usage of the Account Reset Console.
Select 'Access Log' or 'Action Log,' and specify a date range. Then click 'Display Log' to see what users have been doing on the system.

You can select to view access logs (logs of who has logged on or off the Account Reset Console) or action logs (logs of which user accounts have been reset or viewed by which users). Both successful actions and failed requests are logged. For more information, see the “Log Viewing” section of this document.

Configuring Verification Questions and Answers [Advanced]

Before users can use the Account Reset Console to reset their lost passwords via question-and-answer identity verification, you will need to configure the verification questions and answers. To do this you will need to use the **Data Sources**, **Verification**, and **Password Change Features** pages. The Data Sources and Verification pages can be accessed through the “Configuration” main menu link; the Password Change Features page can be accessed through the “Management” main menu link.

You will begin configuring the verification system at the “Verification” side menu tab in the “Configuration” main menu section.



| User Identity Verification Configuration | |
|--|--|
| Data Sources | <p>Configure user identity verification questions here</p> <p>Active Questions:</p> <p>What is your favorite color? [Remove] [Edit]</p> <p>What is your mother's maiden name? [Remove] [Edit]</p> <p>What is your first pet's name? [Remove] [Edit]</p> <p>Inactive Questions:</p> <div><p>Set test user information</p><p>Username <input type="text" value="bob"/></p><p>Domain <input type="text" value="[local]"/> <input type="button" value="v"/></p><p><input type="button" value="Update Test User"/></p></div> <div><p>Add New Question</p><p>Question Text: <input type="text"/></p><p><input type="button" value="Add Question"/></p></div> |
| Log Config | |
| Verification | |
| Domains | |
| Security | |
| Super-Users | |
| Licensing | |
| Add-Ons | |

The Account Reset Console will configure three initial questions for you by default. You can add or remove these questions to/from the list of required questions by clicking the **[Add]** and **[Remove]** links. By default on installation, all three questions are required.

You can add more questions by entering the question text at the bottom of the screen and clicking “Add Question”. You should also take this opportunity to select your test user. This test user account will be used to check the entries in the database to confirm that the system is functioning. It should properly be a member of one of the domains you are managing so that you can test the domain name values stored in your verification databases.

Once you have a list of questions you are happy with, it will be time to edit each question so that it retrieves its answer from the appropriate location. You can access this by clicking the **[Edit]** link.

| User Identity Verification Configuration | |
|---|--|
| <ul style="list-style-type: none"> Data Sources Log Config <li style="background-color: #d3d3d3;">Verification Domains Security Super-Users Licensing Add-Ons | <p>Edit Verification Question</p> <p>Question Text: <input style="width: 90%;" type="text" value="What is your favorite color?"/></p> <p> <input checked="" type="radio"/> Use the Default Database for verification <input type="radio"/> Use custom verification database </p> <p>Data Source: <input style="width: 80%;" type="text" value="Select a data source"/> (Not Working)</p> <p>Queries</p> <p>Retrieval: <input style="width: 90%;" type="text"/> </p> <p style="font-size: small;">If your retrieval query is not working, please ensure that you have records in the appropriate database for your test user.</p> <p><input checked="" type="checkbox"/> Allow users to set their own answers to this question</p> <p>Setting: <input style="width: 90%;" type="text"/> </p> <p>Insertion: <input style="width: 90%;" type="text"/></p> <p>User Deletion: <input style="width: 90%;" type="text"/></p> <p style="text-align: center; margin-top: 10px;"> <input type="button" value="Save Question Settings"/> <input type="button" value="Return to Question List"/> </p> |

The Account Reset Console allows you to design and use your own SQL queries, and thus configure your verification system to access any database you may already be using for data storage. This offers you unparalleled flexibility in verification options.

Once you have finished configuring your questions you will need to make one final change to the password change features, under “Management” on the main menu and “Password Change Features” on the side menu: You need to allow users to reset their forgotten password through ARC via ID verification.

Select the “Allow self service unlock and password reset through ARC (via ID verification)” checkbox. And enter a number of allowable wrong answers (we suggest 3), then click “Save Program Features”. You may also elect to allow self service unlock via ARC Credential Provider which is a separate download and installation for each client. This option allows users

to reset/unlock their accounts without requiring access to a browser or help desk personnel. For further information or to download, please visit the Lieberman Software web site at <http://www.liebsoft.com> and visit the Account Reset Console pages.

The screenshot shows the Lieberman Software Account Reset Console interface. At the top, the user is logged in as 'SECURUS\serviceaccount' with a [Log Out] link. A navigation bar contains 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The main content area is titled 'Manage Password Change Features' and includes a sidebar with links to 'Program Access', 'Group Access', 'Account Reset Features', 'Password Change Features', 'Configure Email Settings', 'Appearance', and 'Mobile Settings'. The 'Password Change Features' section contains a text box explaining that these features are for general users resetting their own passwords. Below this are several checkboxes: 'Allow users to change their own passwords using the web interface' (checked), 'When users change their own passwords, emulate their user account to comply with domain policies' (checked), 'When users change their own passwords, expire them so that they must be changed on next login (ignored when user cannot change password)' (unchecked), 'Allow self service unlock and password reset through ARC (via ID verification)' (checked), and 'Allow self service unlock and password reset through Credential Provider / Gina (via ID verification)' (checked). At the bottom, there are two input fields: 'Verification allowed wrong answers: 3' and 'Verification wrong answers timeout(minutes): 3'.

Once you have completed these steps, you should see that the login screen for the Account Reset Console now includes an option to reset a forgotten or locked-out account:

The screenshot shows the Lieberman Software Account Reset Console login screen. It features the Lieberman Software logo and the title 'Account Reset Console'. The main content area contains the text 'Please log in to access the Account Reset Console.' followed by input fields for 'Username', 'Password', and 'Domain' (set to 'SECURUS'). A 'Log In' button is positioned to the right of the domain field. Below the login fields, there is a link for 'Forgot your password / Locked out?' and a button labeled 'Reset Password / Unlock'.

The new button at the bottom of the login page allows users to answer the selected questions to verify their identity and reset their passwords. You may also notice that the “Set Up My Identity” page becomes available under the “Accounts” main menu item, allowing users to enter their own answers into the database for those questions which allow it:

LIEBERMAN SOFTWARE
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts Scheduling/Reporting Management Configuration Index

Reset User Account

Reset User Account
Look up User Data
Change My Password
Set Up My Identity

Enter Username and a new Password (twice) for the account to be reset.

Username

Domain

Reset the account password

Password

Password (again)

Enable account if disabled

Unlock account if locked

Force user to change password on next login

For more information on configuring user identity information, see “Identity Configuration”, later in this document.

Reviewing Data Security [Advanced]

The Account Reset Console is designed to protect the security of your data sources and network by (a) limiting the amount of time a user automatically stays logged in, and (b) protecting against escape characters in SQL strings before they are sent to your databases. You can modify these settings under the “Configuration” main menu and the “Security” side menu tab.

| Manage Application Security | |
|--|---|
| <ul style="list-style-type: none"> Data Sources Log Config Verification Domains <li style="background-color: #d3d3d3;">Security Super-Users Licensing Add-Ons | <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>These settings allow you to configure the Account Reset Console's security. Change these settings to control how tightly-secured ARCWeb is against unauthorized usage.</p> </div> <p>The session timeout controls how long a web browser session will remain logged-in without activity.</p> <p>Session timeout: <input style="width: 100px;" type="text" value="20"/></p> <p>The allowed character set controls which characters (case-insensitive) will be accepted as valid characters for verification answers.</p> <p>Allowed charset: <input style="width: 300px;" type="text" value="ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890"/></p> <p style="text-align: center; margin-top: 10px;"> <input type="button" value="Save security settings"/> </p> |

When initially evaluating the product, the defaults should suffice. The default character set is designed to protect MS Access and SQL Server databases. For more information on data security, see the “Manage Application Security” section later in this document.

Note that after the last character in the allowed character set screen that there is a space. This is by design and is there to allow users to have spaces in their verification question answers.

Updating the application’s appearance [Advanced]

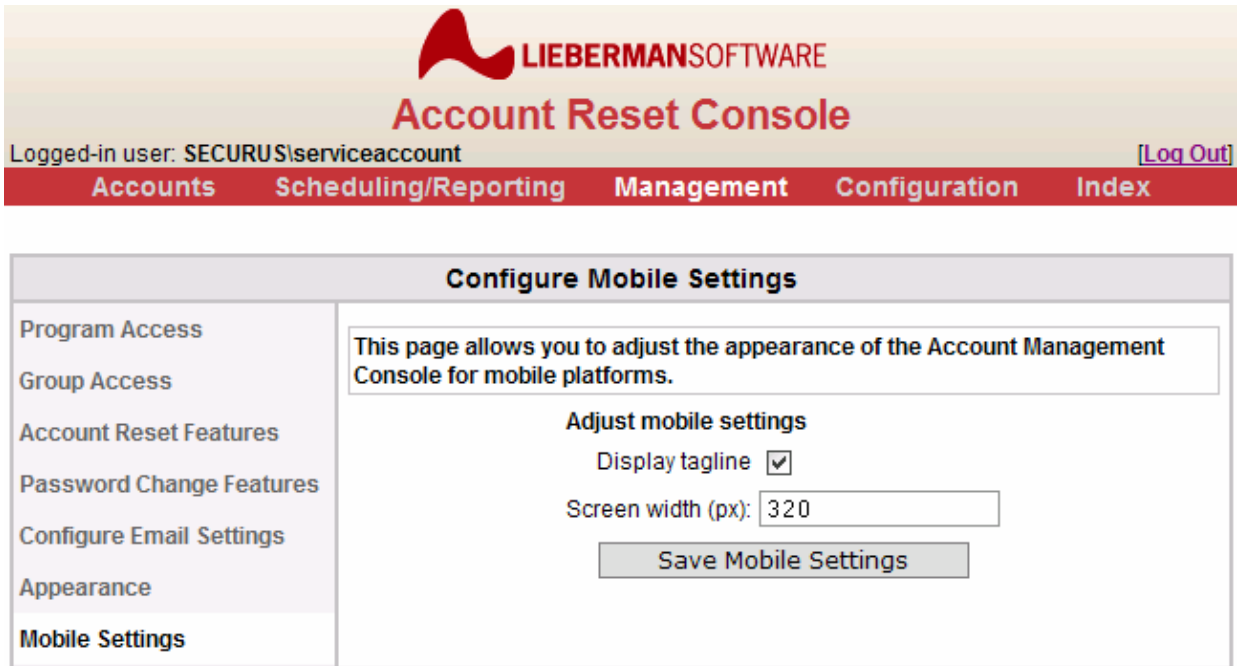
Updating the appearance of the Account Reset Console allows you to incorporate your organization’s colors and logos into the product, thus conveying a unified image to your users. You can change the appearance of the ARCWeb interface under the “Management” main menu and the “Appearance” side menu tab.

| Manage Appearance | |
|--------------------------|--|
| Program Access | <p>This page allows you to adjust the appearance of the Account Management Console. Change these settings to adjust the console to reflect your own organization's brand identity.</p> <p>Adjust appearance settings</p> <p>Company tagline: <input type="text" value="Account Reset Console"/></p> <p>Company Tagline Color: <input type="text" value="C13738"/></p> <p>Select banner image: <input type="text" value="Default Banner (LSC)"/> ▼</p> <p>Upload new banner image (maximum size 640x100): <input type="text"/> <input type="button" value="Browse..."/></p> <hr/> <p>Main Menu Bar Colors</p> <p>Menu Bar Color: <input type="text" value="C13738"/></p> <p>Text Color: <input type="text" value="d0d0d0"/></p> <p>Selected Text Color: <input type="text" value="FFFFFF"/></p> <hr/> <p>Side Menu Bar Colors</p> <p>Menu Color: <input type="text" value="F0F0F0"/></p> <p>Text Color: <input type="text" value="606060"/></p> <p>Selected Text Color: <input type="text" value="000000"/></p> <hr/> <p>Other Colors</p> <p>Page Header Color: <input type="text" value="e0e0e0"/></p> <p>Page Header Text Color: <input type="text" value="000000"/></p> <p>Page Border Color: <input type="text" value="c0c0c0"/></p> <p>Login Box Border Color: <input type="text" value="c0c0c0"/></p> <p>Login Box Color: <input type="text" value="e2e2e2"/></p> <p><input type="button" value="Save Appearance Settings"/></p> <p><input type="button" value="Restore to Default"/></p> |
| Group Access | |
| Account Reset Features | |
| Password Change Features | |
| Configure Email Settings | |
| Appearance | |
| Mobile Settings | |
| | |
| | |
| | |

All colors should be in hexadecimal RGB format. Thus, **red** would be **FF0000** and **green** **00FF00**. All "0" characters should be zeros, not o's. For more information on changing the application's appearance, see "Appearance" later in this document.

Setting up the mobile site [Advanced]

The Account Reset Console's /Mobile site allows you to access any feature of the application from your mobile device with an optimized download size and screen layout. You can change the ARCWeb mobile behavior under the "Management" main menu and the "Mobile Settings" side menu tab.



The screenshot shows the top navigation bar of the Account Reset Console. The logo for Lieberman Software is at the top center, with the text "LIEBERMAN SOFTWARE" and "Account Reset Console" below it. The logged-in user is "SECURUS\serviceaccount" and there is a "[Log Out]" link. The main navigation menu includes "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index".

The "Configure Mobile Settings" page is displayed, featuring a sidebar with the following menu items: "Program Access", "Group Access", "Account Reset Features", "Password Change Features", "Configure Email Settings", "Appearance", and "Mobile Settings". The main content area contains the following text and controls:

This page allows you to adjust the appearance of the Account Management Console for mobile platforms.

Adjust mobile settings

Display tagline

Screen width (px):

Save Mobile Settings

You will need to determine your selected mobile device's width in pixels to view the application. By default, ARCWeb ships with a 320-pixel screen width, which may be too wide for most phone screens. For more information on setting up the mobile site, see the "Configure Mobile Settings" section later in this document.

Scheduling tasks [Advanced]

Users who have "View Console Logs and Task Reports" access privileges can schedule and view management reports, and users who have "Manage All Web Access Controls" privileges can schedule account tasks as well. You can find task scheduling and report viewing in the "Scheduling/Reporting" main menu section.

- *Management Reports* allow users to report on account statuses but prevent them from taking any actions on the accounts found.
- *Account Tasks* allow users to identify accounts and automate account actions.

| Schedule Account Tasks | |
|------------------------------------|---|
| View Logs | <p>Configure scheduled tasks here</p> <p>Active Tasks:</p> <p><input type="checkbox"/> Find Expiring Users [Deactivate] [Del] [Edit]</p> <p><input type="checkbox"/> Find inactive accounts [Deactivate] [Del] [Edit]</p> <p><input type="checkbox"/> Users who have not yet enrolled [Deactivate] [Del] [Edit]</p> <p>Inactive Tasks:</p> <p><input type="button" value="Run Selected Tasks Now"/></p> <div><p>Add New Task</p><p>Task Name: <input type="text"/></p><p>Task Type: <input checked="" type="radio"/> Password Expiration <input type="radio"/> Self Reset Configuration <input type="radio"/> Account Inactivity</p><p><input type="button" value="Add Task"/></p></div> |
| Management Reports | |
| View Reports | |
| Account Tasks | |
| View Task Results | |

The list of active and inactive tasks is visible. Adding a new task to the inactive list is as simple as entering the task name and type and clicking "Add Task". You can activate/deactivate tasks by clicking the **[Activate]** and **[Deactivate]** links next to the task name.

To configure the task, click the **[Edit]** link next to the task name:



Account Reset Console

Logged-in user: SECURUS\serviceaccount

[\[Log Out\]](#)

[Accounts](#) [Scheduling/Reporting](#) [Management](#) [Configuration](#) [Index](#)

Schedule Account Tasks

[View Logs](#)

[Management Reports](#)

[View Reports](#)

Account Tasks

[View Task Results](#)

Edit Scheduled Task

Task Name: Find Expiring Users

Task runs on Sunday Monday Tuesday Wednesday Thursday
 Friday Saturday

at Noon

Last Run: Never ()

Target Groups: SECURUS\domain users [\[del\]](#)

SECURUS

Filter Users: Ignore usernames which contain the following substrings
(separate by ;):

Task Details: Find accounts whose password will expire in days

Disable the user's account

Enable the user's account

Send the user an email

Dear #RealName#,

Your password is about to expire.
Please visit <http://server/arcweb> to
change your password before it expires.

Plain Text Email HTML Email RTF Email

User email keywords:

#RealName# - User's full name as stored in Active Directory.

#PwdDaysToExp# - Days until the user's password expires.

Email results to:

Plain Text Email HTML Email

In the edit screen you can change the interval, which groups and users it scans for, and what actions to take. You can find more information on scheduling tasks in the “Scheduling Tasks and Reports” section later in this document.

Once your scheduled tasks begin to run you will be able to view the reports they generate by clicking the “View Task Results” side menu tab under the “Scheduling/Reporting” main menu section.

Configuring licensing [Advanced]

The final step in getting started is to purchase and enter a valid serial number from Lieberman Software Corporation. Licensing and serial number information is available in the “Configuration” main menu section, under the “Licensing” tab:

The screenshot shows the Lieberman Software Account Reset Console interface. At the top, it displays the Lieberman Software logo and the title "Account Reset Console". Below the title, it indicates the logged-in user as "SECURUS\serviceaccount" and provides a "[Log Out]" link. A navigation bar contains the following menu items: "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index".

The main content area is titled "ARCWeb Licensing" and is divided into two columns. The left column contains a sidebar menu with the following items: "Data Sources", "Log Config", "Verification", "Domains", "Security", "Super-Users", "Licensing", and "Add-Ons". The right column displays "Current License Details" with the following information:

| | |
|----------------------|---|
| ComputerID | DC |
| License | X-XXXXXXXX-XXXXXXXX-XXXXXXXX-X-X-XXXXXXXX |
| ManagedUserCount | [update] |
| ManagedUserTimestamp | 5/31/2007 12:01:01 PM |
| ARCWebBuild | 12/12/2005 12:56:24 PM |
| MaximumUsers | XXX |
| ExpDate | [never] |
| SupportExpDate | 5/16/2012 8:44:08 AM |

Below the license details, there is a text input field containing the placeholder "X-XXXXXXXX-XXXXXXXX-XXXXXXXX-X-X-XXXXXXXX" and an "Update License Key" button.

On this page you can enter new serial numbers as well as see the total number of managed users and the version of the product you currently have installed. The Account Reset Console is licensed based on the number of users you are managing. Any user which is a member of a group that can reset its own passwords or which can be reset by ARCWeb help desk users counts as a managed user.

Changing Your Own Password

Overview

The Account Reset Console can allow users to reset their own passwords.

Self-service password change is located under the “Accounts” menu item, in the “Change My Password” tab. Users with “Allow Web Logon” privileges can reset their own passwords if the Account Reset Console is configured to allow them to do so.

Changing Your Password



The screenshot shows the Lieberman Software Account Reset Console interface. At the top, there is a red header with the Lieberman Software logo and the text "LIEBERMAN SOFTWARE" and "Account Reset Console". Below the header, it says "Logged-in user: SECURUS\serviceaccount" and a "[Log Out]" link. A navigation bar contains the following menu items: "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index". The main content area is titled "Change My Password" and contains a form with the following elements:

| Change My Password | |
|--------------------|---|
| Reset User Account | Please enter your new Password twice to reset it. Username SECURUS\serviceaccount New Password <input type="text"/> Repeat New Password <input type="text"/> <input type="button" value="Change Password"/> |
| Look up User Data | |
| Change My Password | |
| Set Up My Identity | |

To change your own password, you will need to enter the new password twice. If you enter passwords that do not match, you will be prompted to re-enter them so that they match.

If you enter a password that does not conform to the password rules set by your system administrators, the Account Reset Console will not change your password. Please ensure that your new password conforms to the rules set by your system administrators.

Resetting User Accounts

Overview

The Account Reset Console can allow users to reset other user accounts.

User account reset is located under the “Accounts” menu item, in the “Reset User Account” tab. Users with “Allow Reset of Other Users’ Accounts” privileges can reset other users’ accounts, provided that they have permission to reset the appropriate user groups. ARCWeb administrators can grant help desk users the appropriate permissions to reset other users’ accounts.

Resetting Accounts

LIEBERMAN SOFTWARE
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts Scheduling/Reporting Management Configuration Index

Reset User Account

Reset User Account
Look up User Data
Change My Password
Set Up My Identity

Enter Username and a new Password (twice) for the account to be reset.

Username

Domain

Reset the account password

Password

Password (again)

Enable account if disabled

Unlock account if locked

Force user to change password on next login

To reset an account, enter the user’s username and domain, select the appropriate options, and click “Reset Account”.

Not all the options you see above will be available, depending on how your system administrators have configured the Account Reset Console. The user accounts you are permitted to reset may also be restricted.

Account Reset Options

Not all options will necessarily be available, depending on how your system administrators have configured the Account Reset Console. However, the available options will allow you to reset specific components of user accounts.

- **Reset the account password** – check this box to reset the account password. Once you check this box, the “Password” and “Password (again)” fields will be enabled. You must enter the new password twice to ensure that you have made no typographical errors. If the new passwords do not match, no changes will be made to the account.
- **Enabled account if disabled** – check this box to reset the “disabled” flag on the account.
- **Unlock account if locked** – check this box to reset the “locked” flag on the account.
- **Force user to change password on next login** – check this box to force the user to change their password the next time they log onto Windows.

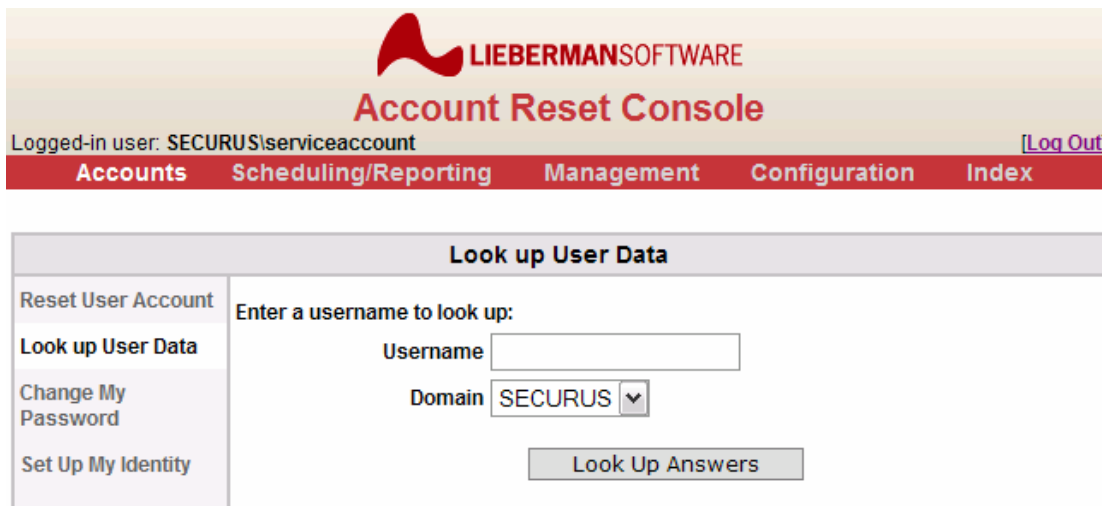
Looking Up User Data

Overview

The Account Reset Console can allow users to view the identity information for another user, preparatory to resetting their account.

User information lookup is located under the “Accounts” menu item, in the “Look up User Data” tab. Users with “Allow Reset of Other Users’ Accounts” privileges can look up other users’ information, provided that they have permission to view the appropriate user groups. ARCWeb administrators can grant help desk users the appropriate permissions to look up other users’ information.

Resetting Accounts



The screenshot displays the Account Reset Console interface. At the top, there is a header with the Lieberman Software logo and the text "LIEBERMAN SOFTWARE Account Reset Console". Below the header, it shows the logged-in user as "SECURUS\serviceaccount" and a "[Log Out]" link. A navigation bar contains the following menu items: "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index". The main content area is titled "Look up User Data" and features a sidebar with links: "Reset User Account", "Look up User Data", "Change My Password", and "Set Up My Identity". The "Look up User Data" section contains a form with the following fields: "Enter a username to look up:", "Username" (text input), "Domain" (dropdown menu showing "SECURUS"), and a "Look Up Answers" button.

To look up user information, enter the user's username and domain and click "Look Up Answers". The user accounts you are permitted to view may be restricted.

The screenshot shows the Lieberman Software Account Reset Console. At the top, there is a logo for Lieberman Software and the title "Account Reset Console". Below the title, it says "Logged-in user: SECURUS\serviceaccount" and a "[Log Out]" link. A navigation bar contains the following items: "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index". The main content area is titled "Look up User Data" and contains a table with the following information:

| Look up User Data | |
|--------------------|---|
| Reset User Account | Identity information for SECURUS\bucky |
| Look up User Data | What is your favorite color? |
| Change My Password | brown |
| Set Up My Identity | What is your mother's maiden name? |
| | bojangles |
| | What is your first pet's name? |
| | dog |
| | <input type="button" value="Reset User Account Now"/> |

The user's identity information will be displayed so that the help desk user can confirm their identity by having the user answer each question. Once the help desk user is done, they can click "Reset User Account Now" to automatically take them to the Account Reset screen and automatically fill in the user's domain and username.

Identity Configuration

Overview

The Account Reset Console can allow users to verify their identity and reset forgotten passwords by answering a series of questions.

Identity configuration is located under the "Accounts" menu item, in the "Set Up My Identity" tab. Identity data can be configured by users with "Allow Web Logon" privileges.

Setting Up Identity Information

LIEBERMAN SOFTWARE
Account Reset Console

Logged-in user: SECURUS\bucky [\[Log Out\]](#)

[Accounts](#) [Index](#)

Set Up My Identity

| | |
|------------------------------------|--|
| Change My Password | Use this page to configure your identity verification data. |
| Set Up My Identity | <p>What is your favorite color? Answer: <input type="text" value="brown"/></p> <p>What is your mother's maiden name? Answer: <input type="text" value="bojangles"/></p> <p>What is your first pet's name? Answer: <input type="text" value="dog"/></p> <p>Your verification information is complete. Your account is properly configured for password recovery.</p> <p><input type="button" value="Save Verification Info"/></p> <p>This page allows you to save your identity verification data. Once you have saved this information, you will be able to reset your password if you forget it by providing the answers to these questions.</p> |

If the Account Reset Console is configured to allow users to verify their identity, and there are questions that the users can supply answers for, users will be given the opportunity to answer these questions on this page. Each user-configurable question will be listed.

To change your answers, simply enter the new value into the “Answer” box below the appropriate question and click “Save Verification Info”. The Account Reset Console will save the new answer to the database provided by your system administrators.

If you have not supplied answers for all of the verification questions, a red message will tell you “**Your verification information is not complete.**” This indicates that you will not be able to use the ID verification system to recover your password until you have supplied answers to ALL of the questions.

The Account Reset Console protects the data sources accessed by the verification system against intrusion by limiting the characters you can enter into the answer fields. In this scenario, you may see a message such as the one below. You will have to use a different answer to proceed.

Set Up My Identity

Use this page to configure your identity verification data.

One or more of your answers contained illegal characters. These answers have not been modified.

Log Viewing

Overview

The Account Reset Console logs all access attempts and account actions, recording the user name, domain, and action taken, including success or failure. These logs can be retrieved by username and/or date.

Log retrieval is located under the “Scheduling/Reporting” menu item, in the “View Log” tab. Logs can be retrieved by users with “View Console Logs and Task Reports” privileges.

Log Viewing Options

The screenshot shows the 'Account Reset Console' interface. At the top, there is a logo for 'LIEBERMAN SOFTWARE' and the title 'Account Reset Console'. Below the title, it says 'Logged-in user: SECURUS\serviceaccount' and a '[Log Out]' link. A navigation bar contains the following items: 'Accounts', 'Scheduling/Reporting' (which is highlighted), 'Management', 'Configuration', and 'Index'. The main content area is titled 'View Account Reset Console Logs'. On the left side, there is a sidebar with the following options: 'View Logs', 'Management Reports', 'View Reports', 'Account Tasks', and 'View Task Results'. The main content area contains the following elements: 'Display Activity Log' with two radio buttons: 'Access Log' (selected) and 'Action Log'; a date range selector showing '5/31/2007' to '5/31/2007'; a 'Username:' label followed by an input field; and a 'Display Log' button. Below these elements, there is a text box with the following instructions: 'Use this screen to report on usage of the Account Reset Console. Select 'Access Log' or 'Action Log,' and specify a date range. Then click 'Display Log' to see what users have been doing on the system.'

The Account Reset Console will display logs from the current logfile. Any logging information saved in a different log data source will not be displayed.

There are two separate logs that the Account Reset Console can display. The first is the *Access Log*, which contains information on which users have accessed (logged onto) the Account Reset Console. The other is the *Action Log*, which contains information on which user accounts have been reset or viewed (or have been attempted to be reset or viewed) by which other users.

Logs can be displayed for a range of dates and can be limited to a single user if desired.

Viewing the Access Log

To view the Access Log, select “Access Log”, enter the desired range of dates and user account, and click “Display Log”.

| View Account Reset Console Logs | | | | |
|--|-------------------------------|---------------|---------------------------|------------------------|
| View Logs Management Reports View Reports Account Tasks View Task Results | Access Log - 5/31/2007 | | | |
| | Date | IP Address | Action | User |
| | 05/31/2007 12:15:21 | 1.1.0.0 | logon success | SECURUS\serviceaccount |
| | 05/31/2007 12:28:19 | 1.1.0.0 | logoff | SECURUS\serviceaccount |
| | 05/31/2007 12:28:37 | 1.1.0.0 | logon success | SECURUS\serviceaccount |
| | 05/31/2007 13:05:23 | 1.1.0.0 | logoff | SECURUS\serviceaccount |
| | 05/31/2007 13:07:20 | 1.1.0.0 | logon success | SECURUS\serviceaccount |
| | 05/31/2007 14:03:22 | 1.1.0.0 | logoff | SECURUS\serviceaccount |
| | 05/31/2007 14:03:35 | 1.1.0.0 | logon failure | SECURUS\bucky |
| | 05/31/2007 14:03:41 | 1.1.0.0 | logon failure | SECURUS\bucky |
| | 05/31/2007 14:03:46 | 1.1.0.0 | logon failure | SECURUS\bucky |
| | 05/31/2007 14:03:59 | 1.1.0.0 | multifactor logon success | SECURUS\bucky |
| | 05/31/2007 14:04:13 | 1.1.0.0 | logoff | SECURUS\bucky |
| | 05/31/2007 14:04:17 | 1.1.0.0 | logon success | SECURUS\bucky |
| | 05/31/2007 14:04:42 | 1.1.0.0 | logoff | SECURUS\bucky |
| | 05/31/2007 14:04:53 | 1.1.0.0 | logon success | SECURUS\serviceaccount |
| | 05/31/2007 14:05:41 | 1.1.0.0 | logoff | SECURUS\serviceaccount |
| 05/31/2007 14:05:46 | 1.1.0.0 | logon success | SECURUS\bucky | |
| 05/31/2007 14:11:17 | 1.1.0.0 | logoff | SECURUS\bucky | |
| 05/31/2007 14:11:32 | 1.1.0.0 | logon success | SECURUS\serviceaccount | |

The Account Reset Console records the time that the access was attempted, the IP address from which the user attempted to log onto the system, the action (“logon success”, “logon failure”, or “logoff”) and the user attempting to take the action.

Clicking on the headers of each column will sort the table by that column.

Viewing the Action Log

To view the Action Log, select “Action Log”, enter the desired range of dates and user account, and click “Display Log”.

| View Account Reset Console Logs | | | | | | |
|---------------------------------|------------------------|------------|----------------------------------|------------------------|---------------|---------------------------------|
| View Logs | Action Log - 5/31/2007 | | | | | |
| Management Reports | Date | IP Address | Action | User | Reset Account | Status |
| View Reports | 05/31/2007 11:55:27 | | Transfer to new logging database | | | Transfer succeeded |
| View Reports | 05/31/2007 11:55:27 | Terminal | Configuring Log DB | Installer | N/A | Successful |
| Account Tasks | 05/31/2007 14:03:17 | 1.1.0.0 | Lookup User Answers | SECURUS\serviceaccount | SECURUS\bucky | Success |
| View Task Results | 05/31/2007 14:04:06 | 1.1.0.0 | Password | SECURUS\bucky | SECURUS\bucky | Success. Server: \DC |
| View Task Results | 05/31/2007 14:04:06 | 1.1.0.0 | SetAccountFlags | SECURUS\bucky | SECURUS\bucky | Setting Flag LockedOut to FALSE |
| View Task Results | 05/31/2007 14:05:00 | 1.1.0.0 | Lookup User Answers | SECURUS\serviceaccount | SECURUS\bucky | Success |

The Account Reset Console records the time that the access was attempted, the IP address from which the user attempted to log onto the system, the action requested, the user requesting the action, the target of the action, and the result. If the user requesting the account action does not have permissions to reset the account, the log will read “Error: Not Allowed”. If the account action fails, the failure cause will be entered into the reset log.

Clicking on the headers of each column will sort the table by that column.

Scheduling Management Reports

Overview

The Account Reset Console includes an automatic report scheduling system which allows you to automatically generate reports on accounts matching specified criteria.

Task scheduling is located under the “Scheduling/Reporting” menu item, in the “Management Reports” tab. Management reports can be scheduled or run by users with “View Console Logs and Task Reports” privileges.

Creating and Viewing Management Reports

The scheduled reports that are currently saved are displayed in a table on the main scheduled tasks screen, as shown below:

| Create Management Reports | |
|---|---|
| View Logs Management Reports View Reports Account Tasks View Task Results | <p>Configure scheduled tasks here</p> <p>Active Tasks:</p> <p><input type="checkbox"/> Passwords that will expire in 14 days [Deactivate] [Del] [Edit]</p> <p>Inactive Tasks:</p> <p><input type="button" value="Run Selected Tasks Now"/></p> <div style="border: 1px solid gray; padding: 5px;"> <p>Add New Task</p> <p>Task Name: <input type="text"/></p> <p>Task Type: <input checked="" type="radio"/> Password Expiration <input type="radio"/> Self Reset Configuration <input type="radio"/> Account Inactivity</p> <p><input type="button" value="Add Task"/></p> </div> |

Management reports are divided into two classes: “Active” and “Inactive” reports. Active reports are in the queue to be run when the task process runs; Inactive reports will never be run unless they are transferred into the “Active” list. You can switch a task from Inactive to Active status by clicking the [**Activate**] link next to its name. Similarly, you can switch a task from Active to Inactive status by clicking on the [**Deactivate**] link next to its name.

Each scheduled task has an interval at which it runs, a set of criteria it scans for, and a set of user groups to scan. All task settings can be found by clicking the task’s [**Edit**] link.

Adding Reports

Adding a report is as easy as entering the new report name, selecting the report type, and clicking the “Add Task” button. The report type will determine how the report selects users from its target groups:

- **“Password expiration”** – Select this report type to search for accounts with passwords due to expire in the specified number of days. This scan searches for accounts whose passwords will be expired by the primary domain controller’s password policy. The date used for calculating the time until expiration in the task is drawn from the clock on the machine running ARCWeb, NOT the domain controller. Thus, any inconsistencies in the system clocks between the primary domain controller and the machine running ARCWeb could cause inaccuracies in detecting the appropriate users.
- **“Self Reset Configuration”** – Select this report type to search for users who have not completed enrollment in the self-service verification questions.

- **“Account inactivity”** – Select this report type to search for accounts which have been inactive (have not logged in) for the specified number of days. Any time a login is recorded on any domain controller that ARC is able to contact, the timestamp will be reset. However, if a domain controller goes offline, this information may be inaccurate, as the timestamps stored on that domain controller will no longer be available. The date used for calculating the time until expiration in the task is drawn from the clock on the machine running ARCWeb, NOT the domain controller. Thus, any inconsistencies in the system clocks between the primary domain controller and the machine running ARCWeb could cause inaccuracies in detecting the appropriate users.

Running Reports Immediately

The Account Reset Console will allow you to run reports immediately through the web interface by checking the report’s checkbox and clicking the “Run Selected Tasks Now” button. This allows you to run reports without waiting for them to run at their scheduled time, or allows you to keep “on-demand” reports in the “Inactive” section and run them whenever required.

Editing Report Settings

Clicking the **[Edit]** link next to a report name will allow you to set the report’s interval, target groups, and criteria.

| Create Management Reports | |
|--|---|
| View Logs Management Reports View Reports Account Tasks View Task Results | <p>Edit Scheduled Task</p> <p>Task Name: Passwords that will expire in 14 days</p> <p>Task runs on <input type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday</p> <p>at <input type="text" value="Midnight"/></p> <p>Last Run: Never ()</p> <hr/> <p>Target Groups: SECURUS\domain users [del]</p> <p><input type="text" value="SECURUS"/> <input type="text" value="Enter group here"/> <input type="button" value="Add Group"/></p> <p>Filter Users: Ignore usernames which contain the following substrings (separate by ;): <input type="text"/></p> <hr/> <p>Task Details: Find accounts whose password will expire in <input type="text" value="14"/> days</p> <p>Email results to: <input type="text" value="yourEmail@yourCo.com"/></p> <p><input checked="" type="radio"/> Plain Text Email <input type="radio"/> HTML Email</p> <p style="text-align: center;"> <input type="button" value="Save Task Settings"/> <input type="button" value="Save Task and Run Now"/> </p> <p style="text-align: center;"><input type="button" value="Return to Task List"/></p> |

- **Task Name** – the name you use to refer to the report task. This name will be stored in the reports database so you can find the task output.
- **Task runs on** – select the days of the week on which the task will run.
- **Last Run** – the last time that the task was run, and the status of the run (success or failure).
- **Target Groups** – the list of groups that the task will scan when run. You can add a new group by entering a groupname into the box and clicking “Add Group”. You can delete a target group by clicking on the **[del]** link next to the groupname.
- **Filter Users** – allows to use create a list of users to ignore when running the reports
- **Task Details** – the task will operate on users who meet these criteria. The task will search for users who meet the criteria selected.
- **Email Results to** – enter an email address in this box will cause the scheduled task system to send a summary email to this email address when the task has been completed.
- **Save Task Settings** – click this to save the task settings.
- **Save Task and Run Now** – click this to save the task settings and run the task immediately.
- **Return to Task List** – click this to return to the list of tasks.


Viewing Management Reports

Overview

The Account Reset Console’s automatic task scheduler allows you to generate reports on any scheduled task and save the reports to the logging database. These reports can be viewed by an admin or help desk manager to discover account issues requiring additional action.

Report viewing is located under the “Scheduling/Reporting” menu item, in the “View Reports” tab. Reports can be viewed by users with “View Console Logs and Task Reports” privileges.

Report Viewing Options

**LIEBERMAN SOFTWARE**
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

[Accounts](#) [Scheduling/Reporting](#) [Management](#) [Configuration](#) [Index](#)

Create Management Reports

| View Logs Management Reports View Reports Account Tasks View Task Results | <p>View Scheduled Task Reports</p> <p>Most Recent Reports: [Refresh List]</p> <table style="width: 100%; border-collapse: collapse;"><thead><tr><th style="text-align: left;"><u>Task Name</u></th><th style="text-align: left;"><u>Report Date</u></th><th style="text-align: left;"><u>Status</u></th></tr></thead><tbody><tr><td style="text-align: left;">Accounts that will expire in 14 days</td><td style="text-align: left;">05/31/2007 14:21:17</td><td style="text-align: left;">All actions were completed successfully.</td></tr><tr><td style="text-align: left;">Passwords that will expire in 14 days</td><td style="text-align: left;">05/31/2007 14:20:10</td><td style="text-align: left;">All actions were completed successfully.</td></tr></tbody></table> <p>Task Reports By Name:</p> <table style="width: 100%; border-collapse: collapse;"><thead><tr><th style="text-align: left;"><u>Task Name</u></th><th style="text-align: left;"><u>Last Run Date</u></th></tr></thead><tbody><tr><td style="text-align: left;">Passwords that will expire in 14 days</td><td></td></tr><tr><td style="text-align: left;">Accounts that will expire in 14 days</td><td></td></tr></tbody></table> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p>Use this screen to view the scheduled task reports.</p><p>Select one of the most recent reports at the top of the screen, or select a task name at the bottom to view all runs of that report.</p></div> | <u>Task Name</u> | <u>Report Date</u> | <u>Status</u> | Accounts that will expire in 14 days | 05/31/2007 14:21:17 | All actions were completed successfully. | Passwords that will expire in 14 days | 05/31/2007 14:20:10 | All actions were completed successfully. | <u>Task Name</u> | <u>Last Run Date</u> | Passwords that will expire in 14 days | | Accounts that will expire in 14 days | |
|---|--|---|--------------------|---------------|--|------------------------|---|---|------------------------|---|------------------|----------------------|---|--|--|--|
| <u>Task Name</u> | <u>Report Date</u> | <u>Status</u> | | | | | | | | | | | | | | |
| Accounts that will expire in 14 days | 05/31/2007 14:21:17 | All actions were completed successfully. | | | | | | | | | | | | | | |
| Passwords that will expire in 14 days | 05/31/2007 14:20:10 | All actions were completed successfully. | | | | | | | | | | | | | | |
| <u>Task Name</u> | <u>Last Run Date</u> | | | | | | | | | | | | | | | |
| Passwords that will expire in 14 days | | | | | | | | | | | | | | | | |
| Accounts that will expire in 14 days | | | | | | | | | | | | | | | | |

Scheduled task reports are saved in the current Account Reset Console log database. Any reports saved to a previous log database will not be available.

The Account Reset Console will display the most recent runs of any management report at the top of the page, and a list of all scheduled management reports at the bottom of the page. You can click on the recent run name to view the report of that run:

| Create Management Reports | | | | | | | | | |
|---|--|----------------|--|---------|---------|---------|-------|----------------|--|
| View Logs | ManagementReports: Accounts that will expire in 14 days Run on: 05/31/2007 14:26:05 All actions were completed successfully. Task Configuration Task Description: Find accounts that expire in 14 days Target Groups: SECURUS\domain users. Task Action(s): build report. | | | | | | | | |
| Management Reports | | | | | | | | | |
| View Reports | | | | | | | | | |
| Account Tasks | | | | | | | | | |
| View Task Results | | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Domain</th> <th>User</th> <th>Actions</th> <th>Results</th> </tr> </thead> <tbody> <tr> <td>SECURUS</td> <td>bucky</td> <td>Match criteria</td> <td>✔ The user's password has already expired.</td> </tr> </tbody> </table> | | Domain | User | Actions | Results | SECURUS | bucky | Match criteria | ✔ The user's password has already expired. |
| Domain | User | Actions | Results | | | | | | |
| SECURUS | bucky | Match criteria | ✔ The user's password has already expired. | | | | | | |

The report shows the name of the task and the date of the run, and then displays a list of the users found, the actions taken, and the result of the action.

You can also click on the name of a report task at the bottom of the report listing to see a list of all runs of that report in the database:

| Create Management Reports | | | | | | | |
|-------------------------------------|---|--|---------------|-------------------------------------|--|-------------------------------------|--|
| View Logs | Select a report date to view: Accounts that will expire in 14 days <table border="0"> <thead> <tr> <th><u>Report Date</u></th> <th><u>Status</u></th> </tr> </thead> <tbody> <tr> <td>05/31/2007 14:24:35</td> <td>All actions were completed successfully.</td> </tr> <tr> <td>05/31/2007 14:21:17</td> <td>All actions were completed successfully.</td> </tr> </tbody> </table> | <u>Report Date</u> | <u>Status</u> | 05/31/2007 14:24:35 | All actions were completed successfully. | 05/31/2007 14:21:17 | All actions were completed successfully. |
| <u>Report Date</u> | | <u>Status</u> | | | | | |
| 05/31/2007 14:24:35 | | All actions were completed successfully. | | | | | |
| 05/31/2007 14:21:17 | | All actions were completed successfully. | | | | | |
| Management Reports | | | | | | | |
| View Reports | | | | | | | |
| Account Tasks | | | | | | | |
| View Task Results | | | | | | | |

From this listing you can select a single run and view the results as above.

Scheduling Account Tasks

Overview

The Account Reset Console includes an automatic task and report scheduling system which allows you to automate basic account monitoring and reset tasks, and to generate reports on accounts matching specified criteria.

Task scheduling is located under the “Scheduling/Reporting” menu item, in the “Account Tasks” tab. Tasks can be scheduled by users with “Manage All Web Access Controls” privileges.

Creating and Viewing Account Tasks

The scheduled account tasks that are currently saved are displayed in a table on the main scheduled tasks screen, as shown below:

| Schedule Account Tasks | |
|------------------------------------|---|
| View Logs | Configure scheduled tasks here Active Tasks: <input type="checkbox"/> Find Expiring Users [Deactivate] [Del] [Edit] <input type="checkbox"/> Find inactive accounts [Deactivate] [Del] [Edit] <input type="checkbox"/> Users who have not yet enrolled [Deactivate] [Del] [Edit] Inactive Tasks: <input type="button" value="Run Selected Tasks Now"/> Add New Task Task Name: <input type="text"/> Task Type: <input checked="" type="radio"/> Password Expiration <input type="radio"/> Self Reset Configuration <input type="radio"/> Account Inactivity <input type="button" value="Add Task"/> |
| Management Reports | |
| View Reports | |
| Account Tasks | |
| View Task Results | |

Scheduled tasks are divided into two classes: “Active” and “Inactive” tasks. Active tasks are in the queue to be run when the task process runs; Inactive tasks will never be run unless they are transferred into the “Active” list. You can switch a task from Inactive to Active status by clicking the **[Activate]** link next to its name. Similarly, you can switch a task from Active to Inactive status by clicking on the **[Deactivate]** link next to its name.

Each scheduled task has an interval at which it runs, a set of criteria it scans for, a set of actions to take on the user accounts it finds, and a set of user groups to scan. All task settings can be found by clicking the task’s **[Edit]** link.

Adding Tasks

Adding a task is as easy as entering the new task name, selecting the task type, and clicking the “Add Task” button. The task type will determine how the task selects users from its target groups:

- **“Password expiration”** – Select this task type to search for accounts with passwords due to expire in the specified number of days. This scan searches for accounts whose passwords will be expired by the primary domain controller’s password policy. The date used for calculating the time until expiration in the task is drawn from the clock on the machine running ARCWeb, NOT the domain controller. Thus, any inconsistencies in the system clocks between the primary domain controller and the machine running ARCWeb could cause inaccuracies in detecting the appropriate users.
- **“Self Reset Configuration”** – Select this report type to search for users who have not completed enrollment in the self-service verification questions.
- **“Account inactivity”** – Select this task type to search for accounts which have been inactive (have not logged in) for the specified number of days. Any time a login is recorded on any domain controller that ARC is able to contact, the timestamp will be reset. However, if a domain controller goes offline, this information may be inaccurate, as the timestamps stored on that domain controller will no longer be available. The date used for calculating the time until expiration in the task is drawn from the clock on the machine running ARCWeb, NOT the domain controller. Thus, any inconsistencies in the system clocks between the primary domain controller and the machine running ARCWeb could cause inaccuracies in detecting the appropriate users.

Running Tasks Immediately

The Account Reset Console will allow you to run tasks immediately through the web interface by checking the task’s checkbox and clicking the “Run Selected Tasks Now” button. This allows you to run tasks without waiting for them to run at their scheduled time, or allows you to keep “on-demand” tasks in the “Inactive” section and run them whenever required.

Editing Task Intervals and Actions

Clicking the **[Edit]** link next to a task name will allow you to set the task’s name, interval, criteria, and actions.



Account Reset Console

Logged-in user: SECURUS\serviceaccount

[\[Log Out\]](#)

[Accounts](#) [Scheduling/Reporting](#) [Management](#) [Configuration](#) [Index](#)

Schedule Account Tasks

[View Logs](#)

[Management Reports](#)

[View Reports](#)

Account Tasks

[View Task Results](#)

Edit Scheduled Task

Task Name: Find Expiring Users

Task runs on Sunday Monday Tuesday Wednesday Thursday
 Friday Saturday

at Noon

Last Run: Never ()

Target Groups: SECURUS\domain users [\[del\]](#)

SECURUS

Filter Users: Ignore usernames which contain the following substrings
(separate by ;):

Task Details: Find accounts whose password will expire in days

Disable the user's account

Enable the user's account

Send the user an email

Dear #RealName#,

Your password is about to expire.
Please visit <http://server/arcweb> to
change your password before it expires.

Plain Text Email HTML Email RTF Email

User email keywords:

#RealName# - User's full name as stored in Active Directory.

#PwdDaysToExp# - Days until the user's password expires.

Email results to:

Plain Text Email HTML Email

- **Task Name** – the name you use to refer to the task. This name will be stored in the reports database so you can find the task output.
- **Task runs on** – select the days of the week on which the task will run.
- **Last Run** – the last time that the task was run, and the status of the run (success or failure).
- **Target Groups** – the list of groups that the task will scan when run. You can add a new group by entering a group name into the box and clicking “Add Group”. You can delete a target group by clicking on the **[del]** link next to the group name.
- **Filter Users** – allows to use create a list of users to ignore when running the reports
- **Task Details** – the task will operate on users who meet these criteria. The task will search for users who meet the criteria selected.
- **Actions** – Once the scheduled task has detected users it will take the specified actions.
 - **“Disable the user’s account”** – check this box to have the scheduled task disable the account. DO NOT select both “Disable account” and “Enable account” on the same task!
 - **“Enable the user’s account”** – check this box to have the scheduled task enable the account. DO NOT select both “Disable account” and “Enable account” on the same task!
 - **“Save the task results to the reports database”** – check this box to save the detected accounts and the actions taken to the reports database. Note that account reset actions are always saved to the log; the reports database is stored separately and is sorted by task and date, not by user account.
 - **“Send the user an email”** – check this box to send an email to the user at his or her Active Directory email address. You may enter the text of the email message in the textarea below this checkbox. You can use wildcards to specify fields to automatically fill in:
 - **#RealName#** - the real name of the user, as stored in Active Directory.
 - **#PwdDaysToExp#** - the days before the user’s password will expire.
 - **#InactiveDays#** - the number of days the user’s account has been inactive.
- **Email Results to** – enter an email address in this box will cause the scheduled task system to send a summary email to this email address when the task has been completed.
- **Save Task Settings** – click this to save the task settings.
- **Save Task and Run Now** – click this to save the task settings and run the task immediately.
- **Return to Task List** – click this to return to the list of tasks.

Viewing Account Task Reports

Overview

The Account Reset Console’s automatic task scheduler allows you to generate reports on any scheduled task and save the reports to the logging database. These reports can be viewed by an admin or help desk manager to discover account issues requiring additional action.

Report viewing is located under the “Scheduling/Reporting” menu item, in the “View Task Results” tab. Reports can be viewed by users with “Manage All Web Access Controls” privileges.

Report Viewing Options

| View Account Task Results | | | | | | | | | | | | |
|--|---|--|------------------|--------------------|---------------|-------------------------------------|---------------------|--|------------------|----------------------|-------------------------------------|--|
| View Logs Management Reports View Reports Account Tasks View Task Results | <p>View Scheduled Task Reports</p> <p>Most Recent Reports: [Refresh List]</p> <table border="1"> <thead> <tr> <th><u>Task Name</u></th> <th><u>Report Date</u></th> <th><u>Status</u></th> </tr> </thead> <tbody> <tr> <td>Find Expiring Users</td> <td>05/31/2007 14:33:55</td> <td>All actions were completed successfully.</td> </tr> </tbody> </table> <p>Task Reports By Name:</p> <table border="1"> <thead> <tr> <th><u>Task Name</u></th> <th><u>Last Run Date</u></th> </tr> </thead> <tbody> <tr> <td>Find Expiring Users</td> <td></td> </tr> </tbody> </table> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Use this screen to view the scheduled task reports.</p> <p>Select one of the most recent reports at the top of the screen, or select a task name at the bottom to view all runs of that report.</p> </div> | | <u>Task Name</u> | <u>Report Date</u> | <u>Status</u> | Find Expiring Users | 05/31/2007 14:33:55 | All actions were completed successfully. | <u>Task Name</u> | <u>Last Run Date</u> | Find Expiring Users | |
| <u>Task Name</u> | <u>Report Date</u> | <u>Status</u> | | | | | | | | | | |
| Find Expiring Users | 05/31/2007 14:33:55 | All actions were completed successfully. | | | | | | | | | | |
| <u>Task Name</u> | <u>Last Run Date</u> | | | | | | | | | | | |
| Find Expiring Users | | | | | | | | | | | | |

Scheduled task reports are saved in the current Account Reset Console log database. Any reports saved to a previous log database will not be available.

The Account Reset Console will display the most recent runs of any scheduled task at the top of the page, and a list of all scheduled task reports at the bottom of the page. You can click on the recent run name to view the report of that run:

| View Account Task Results | | | | | | | | | | |
|--|---|----------------|--|------|---------|---------|---------|-------|----------------|--|
| View Logs Management Reports View Reports Account Tasks View Task Results | <p>AccountTasks: Find Expiring Users Run on: 05/31/2007 14:33:55 All actions were completed successfully.</p> <p>Task Configuration Task Description: Find accounts that expire in 0 days. Target Groups: SECURUS\domain users. Task Action(s): build report.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #800000; color: white;"> <th>Domain</th> <th>User</th> <th>Actions</th> <th>Results</th> </tr> </thead> <tbody> <tr> <td>SECURUS</td> <td>bucky</td> <td>Match criteria</td> <td>✔ The user's password has already expired.</td> </tr> </tbody> </table> | | Domain | User | Actions | Results | SECURUS | bucky | Match criteria | ✔ The user's password has already expired. |
| Domain | User | Actions | Results | | | | | | | |
| SECURUS | bucky | Match criteria | ✔ The user's password has already expired. | | | | | | | |

The report shows the name of the task and the date of the run, a description of the task, a summary, and then a list of the users found, the actions taken, and the result of the action.

You can also click on the name of a scheduled task at the bottom of the report listing to see a list of all runs of that task in the database:

| View Account Task Results | |
|---------------------------|---|
| View Logs | Select a report date to view: |
| Management Reports | Find Expiring Users |
| View Reports | <u>Report Date</u> <u>Status</u> |
| Account Tasks | 05/31/2007 14:33:55 All actions were completed successfully. |
| View Task Results | |

From this listing you can select a single run and view the results as above.

Set Program Access Rights

Overview

User groups can be allowed to login as normal users, allowed to reset other user accounts, and/or allowed to manage the Account Reset Console.

Program access rights are located under the “Management” menu item, in the “Program Access” tab. Program access rights can be managed by users with “Manage All Web Access Controls” privileges.

Program Access Levels

Program access rights are designated at the domain or local group level, not by individual user account name. Any domain or local group may be granted program access rights.

The screenshot shows the 'Account Reset Console' interface. At the top, there is a logo for 'LIEBERMAN SOFTWARE' and the title 'Account Reset Console'. Below the title, it says 'Logged-in user: SECURUS\serviceaccount' and a '[Log Out]' link. A navigation bar contains 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The main content area is titled 'Manage Program Access Permissions'. On the left is a sidebar with menu items: 'Program Access', 'Group Access', 'Account Reset Features', 'Password Change Features', 'Configure Email Settings', 'Appearance', and 'Mobile Settings'. The main area has a section 'Add a New Global Program Access Rule:' with four checkboxes: 'Allow Web Logon', 'Allow Reset of Other Users' Accounts', 'View Console Logs and Task Reports', and 'Manage All Web Access Controls'. To the right of these checkboxes is a 'Domain:' dropdown menu set to 'SECURUS', a text input field 'Enter groupname here', and an 'Add Rule' button. Below this is a table titled 'Global Program Access Rules' with two columns: 'Global Access Category' and 'Allowed Windows Groups'. The table lists several rules with their categories and the groups they apply to, each with a '[del]' link.

| Global Program Access Rules | |
|--------------------------------------|---|
| Global Access Category | Allowed Windows Groups |
| Allow Web Logon | securus\domain admins [del] |
| | SECURUS\can reset [del] |
| | SECURUS\can be reset [del] |
| Manage All Web Access Controls | securus\domain admins [del] |
| Allow Reset of Other Users' Accounts | securus\domain admins [del] |
| | SECURUS\can reset [del] |
| View Console Logs and Task Reports | securus\domain admins [del] |

- **Allow Web Logon** – This access right allows members of the specified group to log onto the Account Reset Console through the web interface.
 - If the Account Reset Console is configured to allow them to change their own passwords, users will have this option once they log in.
 - If the Account Reset Console is configured to allow users to recover passwords through an ID verification process, and there are questions that users need to specify answers for, users will be allowed to set or change their answers once they log in.
- **Allow Reset of Other Users' Accounts** – This access right allows members of the specified group to reset other users' accounts once they log in. Examples of groups who should have this access right might be help desk users or network administrators.
 - Groups with this access right must still be granted group access rights to manage specific groups. For more information, see “Set Group Access Rights”, below.
- **View Console Logs and Task Reports** – This access right allows members of the specified group to schedule tasks, view the Account Reset Console logs, and view the reports generated by scheduled tasks.
- **Manage All Web Access Controls** – This access right allows members of the specified group to manage the application's day-to-day functions.
 - Users with this access right can set program and group access rights for other windows groups.
 - Users with this access right can configure the program features for account reset and password change.
 - Users with this access right can view the system logs.
 - Users with this access right can configure the Account Reset Console's appearance.

Adding Access Rights

To grant program access rights to a Windows group, check the desired access rights, select the domain or local machine as appropriate, enter the name of the group in the edit box, and click “Add Rule”. This will grant the selected program access rights to the specified group. You will see the list of existing access rights change to include the new rights.

Viewing or Deleting Existing Access Rights

The existing group program access rights are listed at the bottom of the page. Any group can be deleted from a given rights list by clicking the “[del]” link next to its name. Deleting a group from any particular rights list removes those rights from the group.

Permission “Stacking”

Each permission level bestows a specific set of capabilities upon the group. It is important to note that these are not inclusive! For example, a group with “Allow Reset of Other Users' Accounts” but not “Allow Web Login” *will not be able to log into the Account Reset Console!*

Set Group Access Rights

Overview

User groups that are allowed to reset other user accounts are strictly limited to resetting only accounts which they are permitted to affect.

Group access rights are located under the “Management” menu item, in the “Group Access” tab. Group access rights can be managed by users with “Manage All Web Access Controls” privileges.

Group Access Rights

Group access rights are designated at the domain or local group level, not by individual user account name. Any domain or local group may be granted group access rights.

The screenshot displays the 'Account Reset Console' interface. At the top, it shows the Lieberman Software logo and the title 'Account Reset Console'. Below this, it indicates the logged-in user is 'SECURUS\serviceaccount' and provides a '[Log Out]' link. A navigation bar contains links for 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The main content area is titled 'Manage Group Access Permissions' and features a sidebar with various settings categories. The primary section is 'Add a New Group Access Rule', which includes fields for 'Administrative Group' and 'Managed Group' (both set to 'SECURUS'), a 'Permissions' section with checkboxes for 'Reset Password' (checked) and 'View User Answers' (unchecked), and an 'Add Group Access Rule' button. Below this are two tables: 'Group Access Rules - Account Reset Privileges' and 'Group Access Rules - View User Answers Privileges'. Both tables have columns for 'Administrative Group' and 'Managed Groups', listing rules such as 'SECURUS\can reset' and 'SECURUS\domain admins' with corresponding 'Managed Groups' like 'SECURUS\can be reset' and 'SECURUS\domain users', each with a delete link.

| Group Access Rules - Account Reset Privileges | |
|---|--|
| Administrative Group | Managed Groups |
| SECURUS\can reset | SECURUS\can be reset [del] |
| SECURUS\domain admins | SECURUS\domain users [del] |

| Group Access Rules - View User Answers Privileges | |
|---|--|
| Administrative Group | Managed Groups |
| SECURUS\can reset | SECURUS\can be reset [del] |
| SECURUS\domain admins | SECURUS\domain users [del] |

If an Administrative Group is granted Access to a Managed Group, members of the Administrative Group will be able to use the Account Reset Console to reset the accounts of users that are members of the Managed Group. For example, in the screenshot above,

members of the “can reset” group are permitted to reset accounts of users in the “can be reset” group.

It is important to note that there are two different types of Group Access Rights:

- **Reset Password** – Granting an Administrative Group Reset Password rights allows the members of the Administrative Group to reset the accounts and passwords of users that are members of the Managed Group.
- **View User Answers** – Granting an Administrative Group View User Answers rights allows the members of the Administrative Group to view the user identity information (i.e. identification answers) of users that are members of the Managed Group.

Adding Access Rights

To grant group access rights to a Windows group, enter the appropriate Administrative Group and Managed Group, select the appropriate checkboxes, and click “Add Group Access Rule”. This will grant access rights to the specified group. You will see the list(s) of existing access rights change to include the new rights.

Viewing or Deleting Existing Access Rights

The existing group access rights are listed at the bottom of the page. Any group can be deleted from a given rights list by clicking the “[del]” link next to its name. Deleting a group from any particular rights list removes those rights from the group.

Group Access Permissions

Even though a particular group has been granted access to manage another group, that does not mean that it will be allowed to reset accounts. The administrative group must be granted Web Logon and Allow Reset rights under Program Access Rights, or won't be able to log onto the Account Reset Console at all!

Set Account Reset Features

Overview

The Account Reset Console can be configured to automatically change account flags during account reset or to allow the resetting user to select which flags to change. It can also be configured to email users account password change notifications.

Account reset settings are located under the “Management” menu item, in the “Account Reset Features” tab. Account reset settings can be managed by users with “Manage All Web Access Controls” privileges.

Account Reset Options

You can change account reset options by selecting the appropriate values and clicking the “Save Program Features” button. Note that the values are not saved until you have clicked the “Save Program Features” button at the bottom of the page.

Manage Account Reset Features

Program Access

Group Access

Account Reset Features

Password Change Features

Configure Email Settings

Appearance

Mobile Settings

These features are for IT personnel resetting arbitrary user accounts. Change these settings to allow the IT personnel to reset user accounts.

Account Reset Features

- Reset passwords through Account Reset Console
- Allow Help Desk to view user identity information

Enable disabled accounts

Always Optional Never

Unlock locked accounts

Always Optional Never

Require that reset passwords be changed on next login (ignored when user cannot change password)

Always Optional Never

- Display the following HTML message to Help Desk personnel resetting accounts

- Email users notifications that the Help Desk has reset their passwords

Dear #RealName#,

This is an automatic notification that your account password has just been changed. You should only be receiving

Plain Text HTML Mail Rich Text

Email keywords:

#RealName# - User's full name as stored in Active Directory.

#UserName# - User's logon name.

#Email# - User's email address as stored in Active Directory.

#Password# - The user's new password.

Save Program Features

- **Reset Password through Account Reset Console** – check this box to allow user passwords to be reset during account reset. If this box is not checked, help-desk users will not be given the option to reset the password during account reset.
- **Allow Help Desk to view user identity information** – check this box to allow access to the “Look Up User Data” menu item. This allows members of Administrative Groups to view the identity verification answers for members of Managed Groups.
- **Enabled disabled accounts** – allows the admin to configure whether or not the “disabled” flag is reset when the account is reset. If set to “Always”, the account is always re-enabled. If set to “Never”, the account is never re-enabled (it stays in whatever state it was in before being reset). If set to “Optional”, the help desk user is given the option to either re-enable it or leave it in the state it was in before being reset.
- **Unlock locked accounts** – allows the admin to configure whether or not the “locked” flag is reset when the account is reset. If set to “Always”, the account is always unlocked. If set to “Never”, the account is never unlocked (it stays in whatever state it was in before being reset). If set to “Optional”, the help desk user is given the option to either unlock it or leave it in the state it was in before being reset.
- **Require that reset passwords be changed on next login** – allows the admin to configure whether or not the “expired” flag is reset when the account is reset. If set to “Always”, the account password is always expired when reset, so that the user has to change the password when they next log in. If set to “Never”, the account is un-expired, so that the user does not have to reset their password when they next log in. If set to “Optional”, the help desk user is given the option to either expire or un-expire the account.
- **Display the following HTML message to Help Desk personnel resetting accounts** – check this box to display an HTML message to Help Desk personnel using the “Reset User Account” page to reset a user account. This message might include warnings, procedural notes, or company policy.
- **Email users notifications that their passwords have been reset** – check this box to send an email to users when their accounts have been reset. You may enter the text of the email message in the textarea below this checkbox. You can use wildcards to specify fields to automatically fill in:
 - **#RealName#** - the real name of the user, as stored in Active Directory.
 - **#UserName#** - the user’s username.
 - **#Email#** - the email address of the user, as stored in Active Directory.
- **Save Program Features** – saves the selections you have made.

Set Password Change Features

Overview

The Account Reset Console can be configured to allow users to change their own passwords, reset their passwords by verifying their identity through a question-and-answer system, and even to alert users (via email) when their passwords are due to expire.

User password change settings are located under the “Management” menu item, in the “Password Change Features” tab. User password change settings can be managed by users with “Manage All Web Access Controls” privileges.

Password Change Options

You can change password change options by selecting the appropriate values and clicking the “Save Program Features” button.

- **Allow users to change their own passwords using the web interface** – Check this box to allow users to log into the Account Reset Console and change their own passwords. Users will still need to be a member of a group with login permissions to the Account Reset Console. If you do not select this checkbox, users clicking “Change My Password” will receive a message that the option has been disabled by their system administrators.
- **When users change their own passwords, expire them so that they must be changed on next login** – By default, if a user changes their own password, the Account Reset Console resets the password expiration date. Checking this box will force the user to reset their password the next time they log into the domain (NOT the next time they log into the Account Reset Console).
- **Allow lost password recovery through ARC (via ID verification)** – Check this box to allow users to answer identifying questions to reset their passwords. Checking this box will cause the “Reset Password” button to appear on the login page of the Account Reset Console.
- **Allowed wrong answers** – The number of verification questions the user can answer incorrectly before a wrong answer causes the verification attempt to fail.
- **Display the following HTML message to users resetting their own passwords** – check this box to display an HTML message to users personnel using the “Change My Password” page to reset their own passwords. This message might include warnings, procedural notes, or company policy.
- **Email users notifications that their passwords have been reset** – Check this box to send a notification email to users when they change their own password. You may enter the text of the email message in the textarea below this checkbox. You can use wildcards to specify fields to automatically fill in:
 - **#RealName#** - the real name of the user, as stored in Active Directory.
 - **#UserName#** - the user’s username.
 - **#Email#** - the email address of the user, as stored in Active Directory.
- **Email the help desk a notification when a user resets their own password** – Check this box to send a notification email to the help desk when any user resets their own password using the Account Reset Console. You can enter the text of the email and the Help Desk email address below the checkbox. You can use wildcards to specify fields to automatically fill in:
 - **#RealName#** - the real name of the user, as stored in Active Directory.
 - **#UserName#** - the user’s username.
 - **#Email#** - the email address of the user, as stored in Active Directory.
- **Save Program Features** – click this button to save the changes you have made.

Note that the values are not saved until you have clicked the “Save Program Features” button.

| Manage Password Change Features | |
|---------------------------------|---|
| Program Access | <p>These features are for general users resetting their own passwords. Change these settings to allow users to update their own account information.</p> <p>Password Change Features</p> <p><input checked="" type="checkbox"/> Allow users to change their own passwords using the web interface</p> <p><input checked="" type="checkbox"/> When users change their own passwords, emulate their user account to comply with domain policies</p> <p><input type="checkbox"/> When users change their own passwords, expire them so that they must be changed on next login (ignored when user cannot change password)</p> <p><input checked="" type="checkbox"/> Allow self service unlock and password reset through ARC (via ID verification)</p> <p><input checked="" type="checkbox"/> Allow self service unlock and password reset through Credential Provider / Gina (via ID verification)</p> <p>Verification allowed wrong answers: <input type="text" value="3"/></p> <p>Verification wrong answers timeout(minutes): <input type="text" value="3"/></p> <p><input type="checkbox"/> Display the following HTML message to users resetting their own passwords</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p><input type="checkbox"/> Email users notifications that their passwords have been reset</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p><input checked="" type="radio"/> Plain Text <input type="radio"/> HTML Mail <input type="radio"/> Rich Text</p> <p><input type="checkbox"/> Email the help desk a notification when a user resets their own password</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p><input checked="" type="radio"/> Plain Text <input type="radio"/> HTML Mail <input type="radio"/> Rich Text</p> <p>Help Desk Address: <input type="text"/></p> <p>Email keywords:</p> <p>#RealName# - User's full name as stored in Active Directory. #UserName# - User's logon name. #Email# - User's email address as stored in Active Directory. #Password# - The user's new password.</p> <p style="text-align: center;"><input type="button" value="Save Program Features"/></p> |
| Group Access | |
| Account Reset Features | |
| Password Change Features | |
| Configure Email Settings | |
| Appearance | |
| Mobile Settings | |
| | |

Configuring Email Settings

Overview

The Account Reset Console can send emails to users notifying them that their accounts have been reset. It can also notify administrators of scheduled task completion and can send emails to users as part of a scheduled task.

Email settings are located under the “Management” menu item, in the “Configure Email Settings” tab. Email settings can be managed by users with “Manage All Web Access Controls” privileges.

Configuring Email

The screenshot displays the 'Account Reset Console' interface. At the top, there is a header with the Lieberman Software logo and the text 'LIEBERMAN SOFTWARE Account Reset Console'. Below the header, a navigation bar shows the user is logged in as 'SECURUS\serviceaccount' and provides a '[Log Out]' link. The main navigation menu includes 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The 'Configure Email Settings' page is active, showing a sidebar with various settings categories: Program Access, Group Access, Account Reset Features, Password Change Features, Configure Email Settings (highlighted), Appearance, and Mobile Settings. The main content area contains a descriptive text box, a section for 'Manage Email Server Settings', and several input fields for 'Server Name', 'Username', 'Password', 'Source Email Address', 'Reply Email Address', and 'Admin Email Address'. A checkbox option is also present: ' This email server requires authentication'. A 'Save Email Configuration' button is located at the bottom of the form.

- **Server Name** – Enter the name of your email server here. The Account Reset Console will use this email (SMTP) server to send emails to users.
- **This email server requires authentication** – Check this box if your email server will require authentication to send email.
- **Username** and **Password** – If your email server requires authentication, enter the username and password here.
- **Source Email Address** – This is the email address from which emails will appear to come. If your email server requires that the source address be in a particular domain, this is the email address that will need to be in said domain.
- **Reply Email Address** – This is the email address which will be set as the “reply-to” address for outgoing emails.
- **Admin Email Address** – This is the email address of the system administrator. The Account Reset Console will send update and report emails to the system administrator at this address.

Appearance

Overview

The Account Reset Console can be fully “skinned” to integrate with your existing network portal infrastructure. You can select colors and company banners to match your own themes.

Console appearance settings are located under the “Management” menu item, in the “Appearance” tab. Appearance settings can be managed by users with “Manage All Web Access Controls” privileges.

Managing the Account Reset Console Appearance

The screenshot displays the 'Account Reset Console' management interface. At the top, there is a header with the Lieberman Software logo and the text 'Account Reset Console'. Below the header, a navigation bar includes 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The 'Management' tab is active. The main content area is titled 'Manage Appearance' and contains a sidebar on the left with options like 'Program Access', 'Group Access', 'Account Reset Features', 'Password Change Features', 'Configure Email Settings', 'Appearance', and 'Mobile Settings'. The 'Appearance' section is selected. The main content area contains a description: 'This page allows you to adjust the appearance of the Account Management Console. Change these settings to adjust the console to reflect your own organization's brand identity.' Below this, there are several sections for adjusting appearance settings: 'Adjust appearance settings' with fields for 'Company tagline' (Account Reset Console), 'Company Tagline Color' (C13738), 'Select banner image' (Default Banner (LSC)), and an 'Upload new banner image' section with a 'Browse...' button. 'Main Menu Bar Colors' includes 'Menu Bar Color' (C13738), 'Text Color' (d0d0d0), and 'Selected Text Color' (FFFFFF). 'Side Menu Bar Colors' includes 'Menu Color' (F0F0F0), 'Text Color' (606060), and 'Selected Text Color' (000000). 'Other Colors' includes 'Page Header Color' (e0e0e0), 'Page Header Text Color' (000000), 'Page Border Color' (c0c0c0), 'Login Box Border Color' (c0c0c0), and 'Login Box Color' (e2e2e2). At the bottom, there are two buttons: 'Save Appearance Settings' and 'Restore to Default'.

Nearly all colors of the Account Reset Console can be altered at any time, as well as the banner and tagline at the top of the page. To change the appearance of the Account Reset Console, change the values in the page and click “Save Appearance Settings”.

Colors

All colors in the Account Reset Console are saved using standard RGB hexadecimal format. This is a six-figure string in the format RRGGBB, where “RR” is the hexadecimal representation of the red component of the color. A few examples:

- Pure black is “000000”
- Pure white is “FFFFFF”
- Pure red is “FF0000”
- Pure green is “00FF00”
- Pure blue is “0000FF”

Altering the Page Header

The top of each page of the Account Reset Console contains an image and a company tagline. By default, these are the Lieberman Software logo and the tagline “Account Reset Console”.

Company tagline:

Company Tagline Color:

Select banner image:

Upload new banner image:

The tagline and tagline color can be changed using the “Company tagline” and “Company Tagline Color” boxes. All colors are saved using standard RGB hexadecimal format.

New banner images can be uploaded by using the “Browse” button to select the image file on your hard drive and then clicking “Save Appearance Settings”. Once you have uploaded the file, its name will appear in the dropdown box labeled “Select banner image”.

Customizing the Main Menu

The main menu bar of the Account Reset Console can be completely customized as well.

Main Menu Bar Colors

Menu Bar Color:

Text Color:

Selected Text Color:

The background color of the menu bar can be changed by entering a new value into the “Menu Bar Color” box. “Text Color” refers to the *inactive* menu options; “Selected Text Color” refers to the *active* menu options. All colors are saved using standard RGB hexadecimal format.

Customizing the Side Menu

The side menu bar of the Account Reset Console can be completely customized.

Side Menu Bar Colors

| | |
|----------------------|-------------------------------------|
| Menu Color: | <input type="text" value="F0F0F0"/> |
| Text Color: | <input type="text" value="606060"/> |
| Selected Text Color: | <input type="text" value="000000"/> |

The background color of the inactive menu elements can be changed by entering a new value into the “Menu Color” box. “Text Color” refers to the *inactive* menu options; “Selected Text Color” refers to the *active* menu options. The active menu option will always have a white background. All colors are saved using standard RGB hexadecimal format.

Customizing the Page Content

Other colors in the Account Reset Console can be customized as well. The border, header, and header text colors of the primary content box can be changed, as well as the color and border color of the initial “login” box.

Other Colors

| | |
|-------------------------|-------------------------------------|
| Page Header Color: | <input type="text" value="e0e0e0"/> |
| Page Header Text Color: | <input type="text" value="000000"/> |
| Page Border Color: | <input type="text" value="c0c0c0"/> |
| Login Box Border Color: | <input type="text" value="c0c0c0"/> |
| Login Box Color: | <input type="text" value="e2e2e2"/> |

“Page Header Color” and “Page Header Text Color” refer to the color of the page title bar and its text, respectively. In the full-page screenshot above, the page title bar is the grey bar titled “Manage Appearance”. “Page Border Color” refers to the color of the border around the page title bar, the side menu, and the page contents.

“Login Box Border Color” and “Login Box Color” refer to the color of the border and the background of the initial login box. All colors are saved using standard RGB hexadecimal format.

Configuring Mobile Settings

Overview

The Account Reset Console has a mobile site (available at the /Mobile subdirectory) which can be configured to match nearly any mobile device's screen available.

Mobile appearance settings are located under the "Management" menu item, in the "Mobile Settings" tab. Mobile settings can be managed by users with "Manage All Web Access Controls" privileges.

Managing the Mobile Settings

The screenshot shows the 'Account Reset Console' interface. At the top, there is a logo for 'LIEBERMAN SOFTWARE' and the title 'Account Reset Console'. Below this, it indicates the user is logged in as 'SECURUS\serviceaccount' and provides a '[Log Out]' link. A navigation menu is visible with options: 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The main content area is titled 'Configure Mobile Settings'. On the left, there is a sidebar with various settings categories, with 'Mobile Settings' selected. The main content area contains a message: 'This page allows you to adjust the appearance of the Account Management Console for mobile platforms.' Below this, there is a section for 'Adjust mobile settings' which includes a 'Display tagline' checkbox (checked) and a 'Screen width (px):' input field containing the value '320'. A 'Save Mobile Settings' button is located at the bottom of this section.

The mobile settings allow you to customize the appearance of the Account Reset Console in the mobile device of your choosing. Different mobile devices have different screen resolutions, so you may want to reconfigure the Account Reset Console for your organization's selected mobile platform.

- **Display tagline** – You can preserve vertical screen space on your mobile device by choosing to not display the tagline on the mobile site.
- **Screen width (px)** – You can configure the horizontal width of the mobile ARC application in pixels here. This width will dictate the maximum width of the screen for most (not all) of the ARC application's pages. Some pages, such as reports, will not display properly at very narrow resolutions and thus require scrolling.
- **Save Mobile Settings** – Click this to save your changes.

Data Sources

Overview

The Account Reset Console can utilize any ADO-compatible data source as an information source for user identity verification or logging. New data sources can be created at any time, and data source settings can be altered to reflect changes in the network configuration.

Data sources are located under the “Configuration” menu item, in the “Data Sources” tab. Data sources can be managed by users with super-user account privileges.

Viewing Available Data Sources

Available data sources are displayed in a table at the top of the page. Each data source has a unique name, a type, and a status.

The screenshot shows the Account Reset Console interface. At the top, there is a header with the Lieberman Software logo and the text "Account Reset Console". Below the header, it says "Logged-in user: SECURUS\serviceaccount" and a "[Log Out]" link. A navigation bar contains the following items: "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index". The main content area is titled "Manage Data Sources". On the left, there is a sidebar with the following menu items: "Data Sources", "Log Config", "Verification", "Domains", "Security", "Super-Users", "Licensing", and "Add-Ons". The main content area contains the following information:

Add or configure data sources here:

| Name | Type | Working | Actions |
|------------------|------------|---------|--------------|
| Default Database | SQL Server | ✓ | [Edit] [del] |

New Data Source

Name:

Type:

- The **name** of the data source is the identifier by which other Account Reset Console components will refer to the data source.
- The **type** of the data source refers to what sort of provider is being accessed. Currently, the Account Reset Console supports three types of data source:
 - “Microsoft Jet”: Refers to a Microsoft Jet data source.
 - “SQLServer”: Refers to a Microsoft SQL Server database (SQL Server 2000 and above).

- “ConnectionStr”: Refers to any other ADO-compatible database. Users must explicitly construct their own ADO connection string for this sort of data source connection (see “Editing a Data Source,” below).
- The **status** of the data source reflects whether or not the Account Reset Console can currently communicate with the data source. The Account Reset Console will not allow you to configure a critical component with a data source that is not functioning. Working data sources are tagged with a green check, nonfunctional data sources with a red X.

How the Account Reset Console tests data sources

The Account Reset Console tests data source access by attempting to use a series of SQL statements to drop, create, write to, and read from a table named “test_table”. If the data source configuration permissions do not allow table creation or destruction, this series of commands will fail, and the data source will be tagged as nonfunctional.

Adding a Data Source

The Account Reset Console allows you to add a new data source by simply entering a name for the new source and clicking “Add New Data Source”.



The screenshot shows a form titled "New Data Source". It has two input fields: "Name:" followed by a text box, and "Type:" followed by a dropdown menu showing "Microsoft Jet". Below these fields is a button labeled "Add New Data Source".

When you click “Add New Data Source”, a new, unconfigured data source will be added to the Account Reset Console. You will see that the new data source is not functional. To make the data source functional, you will need to configure it by clicking the “Edit” link next to it.

Once you add a new data source, you cannot change the name of that data source.

Editing a Data Source

Clicking on the “[Edit]” link next to any data source will allow you to modify the data source’s name and characteristics. Each type of data source has its own characteristics to change.

When you have finished updating the data source’s configuration, click “Save Data Source Settings” to save the data source. This will update the data source and allow you to see whether or not the new settings are working.

When you have finished working with a data source, click “Return to Data Sources” to return to the main Data Sources page.

The Account Reset Console does not currently support DSN connections.

Editing a Microsoft Jet Data Source

Edit Data Source

Name: Test data source

Type: MS Jet

Server Installation:

Database Name:

Status:  Not Working

Save Data Source Settings

Return to Data Sources

Microsoft Jet data sources are characterized by the server installation and database name.

Editing a Microsoft SQL Server Data Source

Edit Data Source

Name: Default Database

Type: SQL Server

Server Installation:

Database Name:

Username:

Password:

Status:  Working

Save Data Source Settings

Return to Data Sources

A Microsoft SQL Server 2000 data source is characterized by a SQL Server installation, a database name, a username, and a password. The Account Reset Console will attempt to connect to the named database on the named database server, using the username/password pair to authenticate.

Editing a General ADO-Compatible Data Source

Edit Data Source

Data source name: Alternate Log
Type: ConnectionStr

Connection String:

Status: ● Not Working

General ADO-Compatible data sources are characterized by an explicit connection string. You can enter your own connection string, allowing you to connect to any general ADO-compatible database.

Logging Configuration

Overview

The Account Reset Console can utilize any ADO-compatible data source as a log location.

Logging configuration is located under the “Configuration” menu item, in the “Log Config” tab. The logging configuration can be managed by users with super-user account privileges.

Viewing the Log Configuration

The logging database and its current status is shown on the tab:

| Configure ARCWeb Logging | |
|---|---|
| <ul style="list-style-type: none"> Data Sources <li style="background-color: #d3d3d3;">Log Config Verification Domains Security Super-Users Licensing Add-Ons | <p style="text-align: center;">Select the logging database information below</p> <p style="text-align: center;">Logging Data Source: <input style="width: 150px;" type="text" value="Default Database"/> ▼</p> <p style="text-align: center;">Current Settings</p> <p style="text-align: center;"> Name Default Database Type SQL Server Status ✔ Working </p> <p style="text-align: center; margin-top: 10px;"> <input style="width: 200px;" type="button" value="Update logging settings"/> </p> |

Changing the Log Database

You can select any working data source to set as the logging database. The Account Reset Console will not allow you to select a data source that it cannot confirm as functional.

Once you select a logging data source in the drop-down box, click “Update logging settings” to save it. The Account Reset Console will attempt to log test messages to the data source you have selected. If the test logging is successful, the Account Reset Console will begin logging to the new data source; if not, no change will be made.

Log Requirements

The Account Reset Console logs to any SQL Server database. This can be a full installation of SQL Server 2000 or 2005, or MSDE or SQL Express.

User Verification Configuration

Overview

The Account Reset Console can be configured to allow users to reset their own passwords if they have forgotten them. Users answer a series of preconfigured questions correctly to verify their identity, and then are permitted to change their own password. Each question draws from a defined data source to

User verification configuration is located under the “Configuration” main menu item, in the “Verification” tab. The verification configuration can be managed by users with super-user account privileges.

Adding and Removing Questions

The questions currently being used for verification purposes are listed at the top of the “Verification” page.

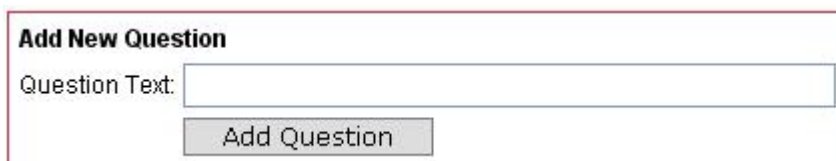
The screenshot displays the Lieberman Software Account Reset Console interface. At the top, the logo and name 'LIEBERMAN SOFTWARE' are shown in red, followed by 'Account Reset Console' in a larger red font. Below this, the logged-in user is identified as 'SECURUS\serviceaccount' with a '[Log Out]' link. A navigation bar contains links for 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration' (which is highlighted), and 'Index'. The main content area is titled 'User Identity Verification Configuration'. On the left is a sidebar menu with options: 'Data Sources', 'Log Config', 'Verification' (selected), 'Domains', 'Security', 'Super-Users', 'Licensing', and 'Add-Ons'. The main panel contains the following sections:

- Configure user identity verification questions here**
- Active Questions:**
 - What is your favorite color? [Remove] [Edit]
 - What is your mother's maiden name? [Remove] [Edit]
 - What is your first pet's name? [Remove] [Edit]
- Inactive Questions:**
- Set test user information**
 - Username:
 - Domain: (dropdown menu)
 -
- Add New Question**
 - Question Text:
 -

Questions are divided into “asked” and “unasked” groups; “asked” questions must be answered by users to verify their identity, while “unasked” questions are not utilized for verification. You can use the “[add]” and “[remove]” links to move questions from “unasked” to “asked” status or vice versa.

New questions can be added to the “unasked” list by entering the question text in the “Add New Question” box and clicking “Add Question”. Newly-added questions will not be

configured. (See “Editing Question Configurations” for details.) Once you have configured a question you can add it to the “asked” list.



Add New Question

Question Text:

Setting the Test User

A test user account is necessary to determine whether or not the questions have been correctly configured. Setting the test user allows the Account Reset Console to set and retrieve answers from your chosen data source for each question, thus confirming that each question is ready to be used for verification.

You set the test user by entering the username and the appropriate domain and clicking “Save Test User Settings”. The Account Reset Console will use this domain and username to test each question’s setting and retrieval syntax (for details, see “Editing Question Configurations,” below).



Set test user information

Username

Domain

Editing Question Configurations

Before any question can be used to verify a user’s identity, it must be configured to set and retrieve the appropriate answer for that user from a valid data source. The Account Reset Console ships with a default verification database which requires users to enroll by entering their own answers into the application; however, advanced users can configure the tool to use custom verification databases which may or may not be pre-populated with user answers (i.e. HR databases). When using custom databases, the Account Reset Console supports any ADO-compatible data source which can be accessed via SQL for purposes of verification. It is up to the site administrator to properly create the verification query strings while configuring each question.

| User Identity Verification Configuration | |
|--|---|
| Data Sources | <p>Edit Verification Question</p> <p>Question Text: <input type="text" value="What is your favorite color?"/></p> <p><input checked="" type="radio"/> Use the Default Database for verification</p> <p><input type="radio"/> Use custom verification database</p> <p>Data Source: <input type="text" value="Select a data source"/> (⚠ Not Working)</p> <p>Queries</p> <p>Retrieval: <input type="text"/> ⚠</p> <p>If your retrieval query is not working, please ensure that you have records in the appropriate database for your test user.</p> <p><input checked="" type="checkbox"/> Allow users to set their own answers to this question</p> <p>Setting: <input type="text"/> ⚠</p> <p>Insertion: <input type="text"/></p> <p>User Deletion: <input type="text"/></p> <p><input type="button" value="Save Question Settings"/></p> <p><input type="button" value="Return to Question List"/></p> |
| Log Config | |
| Verification | |
| Domains | |
| Security | |
| Super-Users | |
| Licensing | |
| Add-Ons | |

The default value for each question is “Use built-in verification database”. When this setting is selected, all other values (data source, query text) are ignored and the Account Reset Console uses the default, built-in SQL Server database to store user enrollment data.

When “Use custom verification database” is selected, the Account Reset Console will attempt to connect to the specified data source and use the retrieval query to get the answer to the question or the setting query to set the answer. There are four queries that you may need to specify, depending on your data source: **retrieval**, **setting**, **insertion**, and **user deletion**.

Verification Query Types

Each verification question may require up to four types of query. The Account Reset Console ships with default query language for all four of these queries.

Retrieval queries are required for all verification questions. This query is used by the Account Reset Console to obtain the user’s verification answer from the database so that ARCWeb can compare it to the entered answer.

Setting queries are only required for verification questions whose answers can be set by the user. If the “Allow users to set their own answers to this question” checkbox is not checked,

you do not need to enter a setting query. If this checkbox is checked, you will need to enter a setting query. The Account Reset Console uses this query to set the answer in the database when the user configures his identity verification answers.

Insertion queries are only required for verification questions whose answers can be set by the user. If the “Allow users to set their own answers to this question” checkbox is not checked, you do not need to enter an insertion query. If this checkbox is checked, you will need to enter an insertion query. The Account Reset Console uses this query to add a user to the database when an appropriate entry for that user does not exist.

User deletion queries are only required for verification questions accessing databases which should be “cleaned up” periodically, that is, have inactive or nonexistent accounts removed. The Account Reset Console currently does not utilize this query.

Designing Queries

Queries should be in SQL. Before the Account Reset Console sends the query language to the data source, it will perform the following substitutions in the query string:

| String | Replaced With | Example |
|------------|-------------------------------|--------------------------------------|
| #user# | The username (without domain) | bob |
| #domain# | The user’s domain | SALESDMN |
| #question# | The GUID of the question | 3C1D8B25-D423-419B-AD6E-E78169B89374 |
| #answer# | The text of the answer | Blue |

When the Account Reset Console performs this replacement, it does not insert (or remove) quotation marks or other tokenizers. Thus, if you have a character-valued column and you want to look up the user name in that column, you will probably have to enclose the #user# in quotes:

```
...where user_name_column = '#user#'...
```

When retrieving the answer from the data source using the retrieval query, it will take the value in the first column of the first row of the retrieved recordset as the answer to the question. You may return any number of rows or columns, but only the first cell will be utilized by the Account Reset Console.

When you click “Save Question Settings,” the Account Reset Console will attempt to retrieve the answer for the specified test user from the data source you have selected, using the retrieval query you have entered. It will also attempt to set that user’s answer, using a predefined test value.

If you have selected the checkbox “Allow users to set their own answers to this question,” users will be allowed to enter an answer to the question in the “Set Up My Identity” tab (described earlier in the document). Users will only be prompted to enter answers to questions

which have this checkbox checked. This allows you to use a mixture of pre-answered and user-configurable questions to verify user identities.

Domain Configuration

Overview

The Account Reset Console can manage multiple domains simultaneously.

Domain configuration is located under the “Configuration” menu item, in the “Domains” tab. The domain configuration can be managed by users with super-user account privileges.

Managing Domains

The list of domains that can be accessed from the local computer is displayed in the “Domains” tab:

The screenshot shows the Account Reset Console interface. At the top, there is a header with the Lieberman Software logo and the text "Account Reset Console". Below the header, it shows the logged-in user as "SECURUS\serviceaccount" and a "[Log Out]" link. A navigation bar contains the following items: "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index".

The main content area is titled "Manage Domains" and contains a sidebar on the left with the following menu items: "Data Sources", "Log Config", "Verification", "Domains", "Security", "Super-Users", "Licensing", and "Add-Ons".

The main content area displays a table titled "Managed Domains and Domain Controllers" with a "Show All" link. The table has the following columns: "Managed Domain", "Primary Domain Controller", "Manage", "Status", and an empty column. The table contains two rows:

| Managed Domain | Primary Domain Controller | Manage | Status | |
|----------------|---------------------------|-------------------------------------|--------|---------------------------|
| SECURUS | DC | <input checked="" type="checkbox"/> | ✓ | [details] |
| [local system] | | <input checked="" type="checkbox"/> | ✓ | |

Below the table, there is a "Default Domain:" label and a "Domain" dropdown menu with "SECURUS" selected. A "Save Domain Configuration" button is located below the dropdown menu.

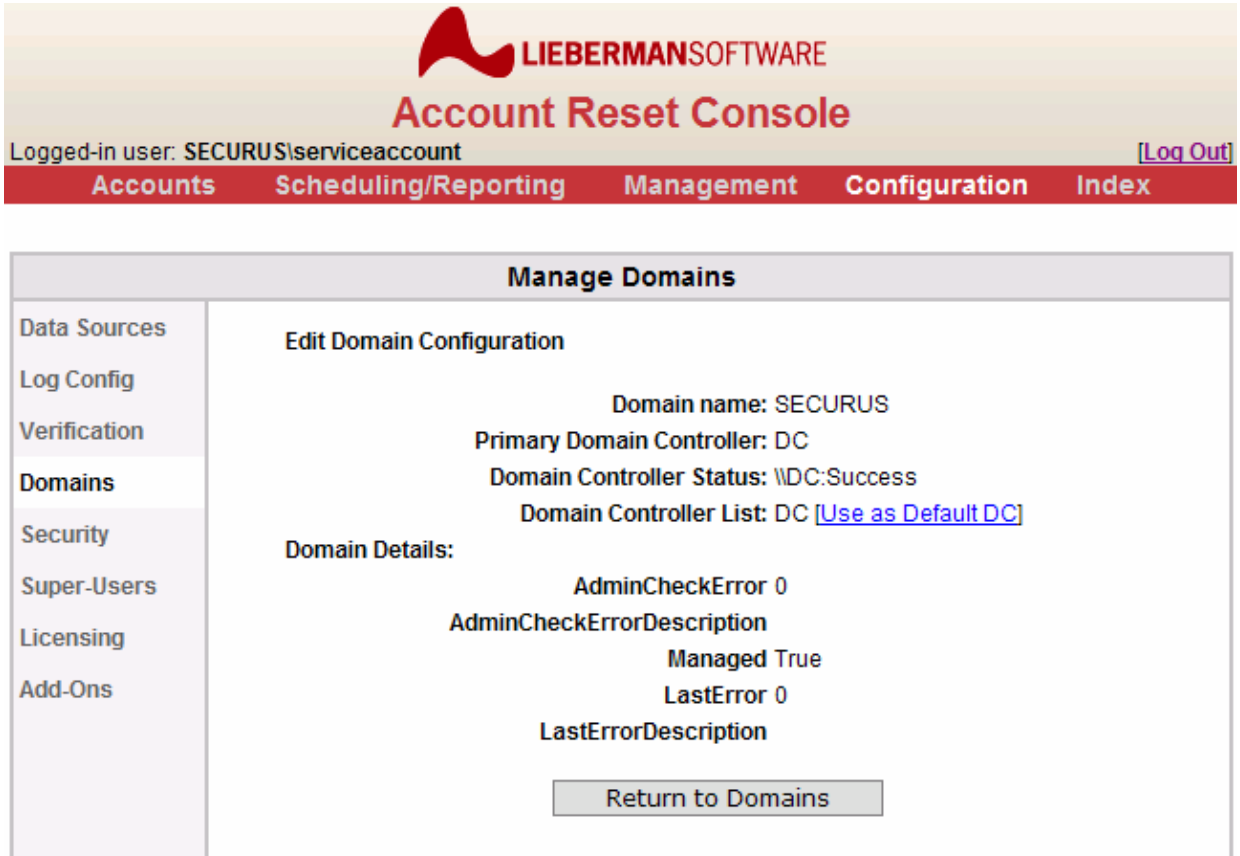
A text box at the bottom of the main content area contains the following text: "Use this screen to set the domains controlled by the Account Management Console."

To manage a domain, the user account being used to run the COM+ application must have administrator privileges on that domain.

To select which domains are managed by the Account Reset Console, check or uncheck the boxes and click “Save Domain Configuration.” If you uncheck all the boxes, the Account Reset Console will still process logins from the local system.

Viewing Domain Details

Clicking the **[details]** link next to a domain name will allow you to view details on that domain.



The screenshot displays the 'Account Reset Console' interface. At the top, there is a logo for 'LIEBERMAN SOFTWARE' and the title 'Account Reset Console'. Below the title, it shows the logged-in user as 'SECURUS\serviceaccount' and a '[Log Out]' link. A navigation bar contains links for 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. The main content area is titled 'Manage Domains' and features a sidebar with navigation options: 'Data Sources', 'Log Config', 'Verification', 'Domains', 'Security', 'Super-Users', 'Licensing', and 'Add-Ons'. The 'Domains' section is active, showing 'Edit Domain Configuration' for the domain 'SECURUS'. The configuration details include: 'Domain name: SECURUS', 'Primary Domain Controller: DC', 'Domain Controller Status: \DC:Success', and 'Domain Controller List: DC [Use as Default DC]'. Under 'Domain Details', the following information is displayed: 'AdminCheckError 0', 'AdminCheckErrorDescription', 'Managed True', 'LastError 0', and 'LastErrorDescription'. A 'Return to Domains' button is located at the bottom of the configuration area.

If there are multiple domain controllers available, you can set ARC to use a preferred domain controller. This is desirable for directing traffic to the nearest domain controller.

Setting the Default Domain

The default domain is the domain which the login domain selection boxes default to. It can be set by selecting the appropriate domain under “Default Domain:” and clicking the “Save Domain Configuration” button.

Application Security

Overview

The Account Reset Console is a password management application and as such must be security-aware. ARCWeb is capable of protecting you against SQL injection attacks and unauthorized web access by allowing you to control your own timeout parameters and permissible character sets.

Security configuration is located under the “Configuration” menu item, in the “Security” tab. The security configuration can be managed by users with super-user account privileges.

Managing Application Security

The screenshot shows the Account Reset Console interface. At the top, there is a header with the Lieberman Software logo and the text "LIEBERMAN SOFTWARE Account Reset Console". Below the header, it says "Logged-in user: SECURUS\serviceaccount" and a "[Log Out]" link. A navigation bar contains the following menu items: "Accounts", "Scheduling/Reporting", "Management", "Configuration", and "Index". The main content area is titled "Manage Application Security" and contains a sidebar with the following options: "Data Sources", "Log Config", "Verification", "Domains", "Security", "Super-Users", "Licensing", and "Add-Ons". The "Security" option is selected. The main content area contains the following text: "These settings allow you to configure the Account Reset Console's security. Change these settings to control how tightly-secured ARCWeb is against unauthorized usage." Below this text, there is a section for "Session timeout" with a description: "The session timeout controls how long a web browser session will remain logged-in without activity." and a text input field containing the value "20". Below this, there is a section for "Allowed charset" with a description: "The allowed character set controls which characters (case-insensitive) will be accepted as valid characters for verification answers." and a text input field containing the value "ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890". At the bottom of the main content area, there is a "Save security settings" button.

The Account Reset Console allows you to specify your own settings for application security without having to modify your web server installation.

- **Session timeout** – This is the number of minutes before the web server will expire the session object which it uses to track a user’s login session. When the session expires the application will automatically log the user out when they next click on a link or

button. The default timeout period is 20 minutes, but if you have a need to make your environment more secure, you can set this as low as 1 minute.

- **Allowed charset** – This is the set of characters (case insensitive) which are acceptable in user-defined answers. Both the answer configuration and identity verification login will use this set to filter the answers before performing any queries to the database. This prevents SQL injection attacks and use of SQL escape characters in the answer strings. By default, this includes the letters A-Z, the number 0-9, and the space character.

The Account Reset Console also protects you from other malicious attacks in the following automatic ways:

- **Sessions, not cookies** – ARCWeb uses only server-side sessions to store login information, not client-side cookies. Names and passwords are not transmitted repeatedly over the network.
- **Entirely SSL-capable** – ARCWeb can be run on a secure HTTP (HTTPS) web server. This will protect all network communications from interception.
- **Server-side answer verification** – All user-provided answer strings are checked in the application logic, not transmitted to the database. Thus, your source databases are protected against SQL injection attacks.

Super-User Configuration

Overview

Super-Users, or users who can access the “Configuration” menu in the Account Reset Console, are not set by normal administrators. These users must be set through the Super-User configuration screen. Super-Users have all access rights to the console, although they do not necessarily have any reset rights for other groups (see “Managing Group Access Rights”, above).

Super-User configuration is located under the “Configuration” menu item, in the “Super-Users” tab. The Super-User configuration can be managed by users with super-user account privileges.

Adding new Super-User Groups

Super-Users are designated at the domain or local group level, not by individual user account name. Any domain or local group may be designated as a super-user group.

The group(s) which are granted super-user access will be able to configure the properties of ARC such as database, logging, and verification question information.



Account Reset Console

Logged-in user: SECURUS\serviceaccount

[\[Log Out\]](#)

[Accounts](#) [Scheduling/Reporting](#) [Management](#) [Configuration](#) [Index](#)

| Manage Super-User Groups | | | | | |
|--------------------------|--|---|------------------------|--------------------------|---|
| Data Sources | <p>Add a new application superuser group:</p> <p>SECURUS <input type="text" value="Enter groupname here"/></p> <p><input type="button" value="Add SuperUsers"/></p> <p>Global Program Access Rules</p> <table border="1"><thead><tr><th>Global Access Category</th><th>Allowed Windows Groups</th></tr></thead><tbody><tr><td>Allow application config</td><td>securus\domain admins [del]</td></tr></tbody></table> <p>Use this screen to grant complete application-control access to members of Windows Groups.</p> | Global Access Category | Allowed Windows Groups | Allow application config | securus\domain admins [del] |
| Global Access Category | | Allowed Windows Groups | | | |
| Allow application config | | securus\domain admins [del] | | | |
| Log Config | | | | | |
| Verification | | | | | |
| Domains | | | | | |
| Security | | | | | |
| Super-Users | | | | | |
| Licensing | | | | | |
| Add-Ons | | | | | |

To add a Super-User group, select the domain or local machine as appropriate, enter the name of the group in the edit box, and click “Set Group as SuperUsers”. This will add the windows group to the list of groups allowed super-user access to the Account Reset Console.

Viewing or deleting existing Super-User Groups

At the bottom of the page are the existing Super-User groups. Any group can be deleted from the list by clicking the “[del]” link next to its name. Deleting a group from the list removes its super-user status.

Super-User Permissions

Users with Super-User permissions are able to access any page of the Account Reset Console. They have no limitations on the changes they can make to the application’s configuration or installation settings.

However, Super-User permissions does not automatically confer upon a user the rights to reset or change another user’s account. This must still be set manually using the “Group Access” tab under “Manage Application”.

Licensing

Overview

The Account Reset Console requires a valid license from Lieberman Software Corporation to run. The Licensing page allows you to view the current license details as well as reset the license in the event of an upgrade or new license purchase.

Licensing is located under the “Configuration” menu item, in the “Licensing” tab. Licensing can be managed by users with super-user account privileges.

Changing or Viewing License Information

Any super-user can view the current license information or enter a new license:

LIEBERMAN SOFTWARE
Account Reset Console

Logged-in user: SECURUS\serviceaccount [\[Log Out\]](#)

Accounts **Scheduling/Reporting** **Management** **Configuration** **Index**

ARCWeb Licensing

| | | |
|------------------|--------------------------------|---|
| Data Sources | Current License Details | |
| Log Config | ComputerID | DC |
| Verification | License | X-XXXXXXXX-XXXXXXXX-XXXXXXXX-X-X-XXXXXXXX |
| Domains | ManagedUserCount | [update] |
| Security | ManagedUserTimestamp | 5/31/2007 12:01:01 PM |
| Super-Users | ARCWebBuild | 12/12/2005 12:56:24 PM |
| Licensing | MaximumUsers | XXX |
| Add-Ons | ExpDate | [never] |
| | SupportExpDate | 5/16/2012 8:44:08 AM |

X-XXXXXXXX-XXXXXXXX-XXXXXXXX-X-X-XXXXXXXX

[Update License Key](#)

To enter a new license, simply copy and paste it into the entry blank (replacing the existing license, if any) and click “Update License Key”.

Licensing is updated twice a day at 12:01 AM and 12:01 PM. It is also updated when you click the UPDATE link or input a new license.

The Account Reset Console is licensed according to the number of users the system is being used to manage. A user is being managed if:

- They have the rights to log into the Account Reset Console and change their own password, or
- Another user can log into the Account Reset Console and reset their account.

If you make changes to group membership that result in too many users being managed, the Account Reset Console may stop working or give you an alert message. If this occurs, you can contact Lieberman Software Corporation for a license upgrade, or you can remove users. To force the Account Reset Console to refresh its user count, click the **[upgrade]** link next to the "ManagedUserCount" entry.

The ARCWeb Site Index

Overview

The Account Reset Console has an index page on the far right of the main menu which shows you every page in the application. This is for your convenience in navigating the application.

The screenshot shows the top of the Account Reset Console. At the top center is the Lieberman Software logo, a red stylized 'L' shape, followed by the text 'LIEBERMAN SOFTWARE' in red. Below this is the title 'Account Reset Console' in a larger red font. Underneath the title, it says 'Logged-in user: SECURUS\serviceaccount' on the left and a '[Log Out]' link on the right. A dark red navigation bar contains five menu items: 'Accounts', 'Scheduling/Reporting', 'Management', 'Configuration', and 'Index'. Below this bar is a white box with a grey header titled 'Index'. The box contains a table with four main categories: 'Accounts', 'Scheduling/Reporting', 'Management', and 'Configuration'. Each category has a list of sub-links.

| Index | |
|-----------------------------|---|
| Accounts | Reset User Account Look up User Data Change My Password Set Up My Identity |
| Scheduling/Reporting | View Logs Management Reports View Reports Account Tasks View Task Results |
| Management | Program Access Group Access Account Reset Features Password Change Features Configure Email Settings Appearance Mobile Settings |
| Configuration | Data Sources Log Config Verification Domains Security Super-Users Licensing Add-Ons |

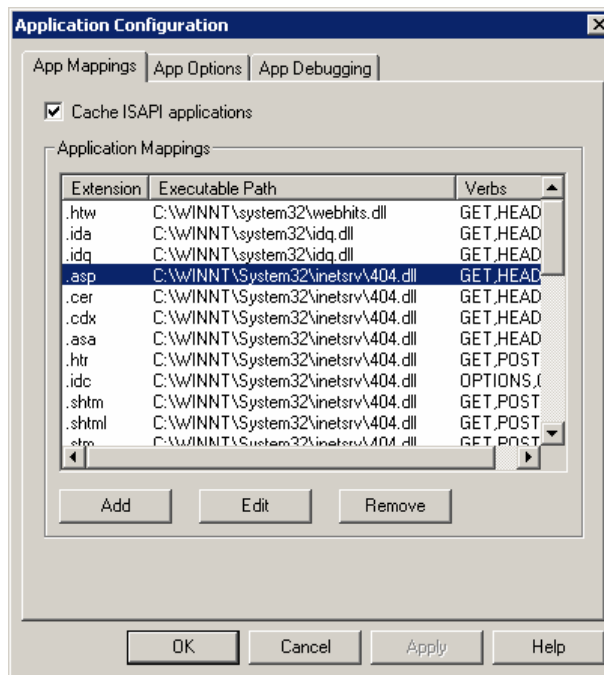
Users will see index entries appropriate for their access level. Thus, only super-users and admins will see the “Management” entries, and only super-users will see the “Configuration” part of the table.

Appendix A

Troubleshooting

Q: When you attempt to access the web page, you receive the error: “Object Disabled”.

A: This error is caused by ASP processing being disabled. This can be corrected by bringing up the properties of the ArcWeb site, clicking on the “Home Directory” tab, click on the “Configuration” button, and enabling the use of the asp.dll file for .asp processing.



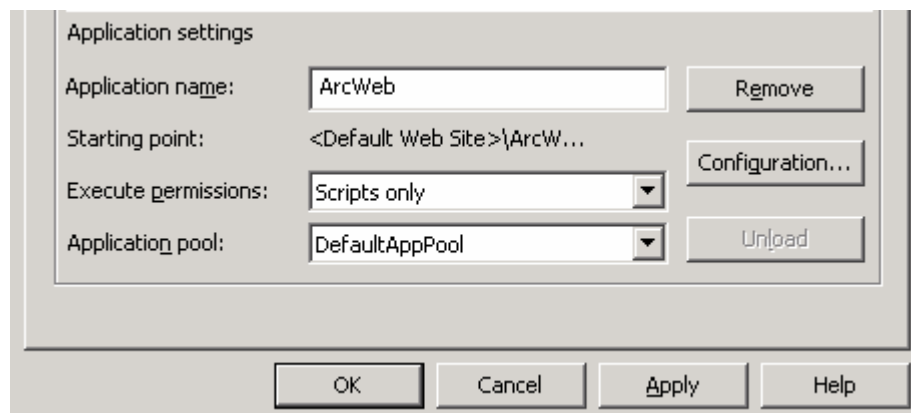
Q: After installation and web site configuration, logon screen is displayed successfully. When a logon is attempted, the message: “Error: Database Not Available”.

Account Reset Console Error: Database Not Available
The Account Reset Console could not access the log database.
Please notify your system administrator of this error.

A: This error is caused by the application not being able to access the SQL Server database where the log is being kept. You may need to double-check your SQL Server credentials in the Admin Console to ensure that they are correct.

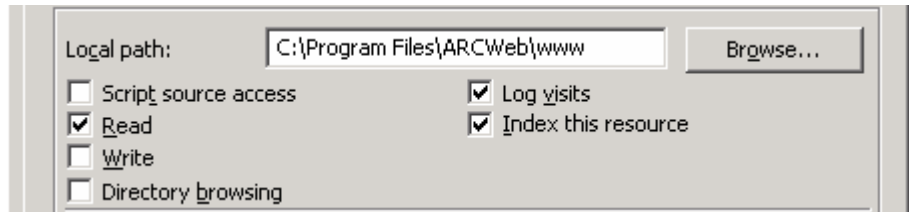
Q: When attempting to load the web site, you receive the following error: “**The page cannot be displayed**” followed by a **403.1** error.

A: Script processing has been disabled. Set **Execute Permission** to “**Scripts only**”.

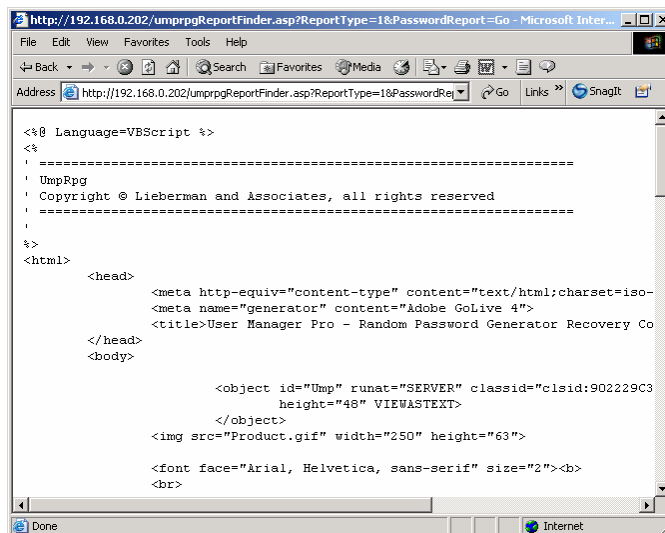


Q: When attempting to load the web site, you receive the following error: “**The page cannot be displayed**” followed by a **403.2** error.

A: This is caused when the “**Home Directory**” permissions are missing the “**Read**” permission. Set the checkbox for “**Read**” permission.

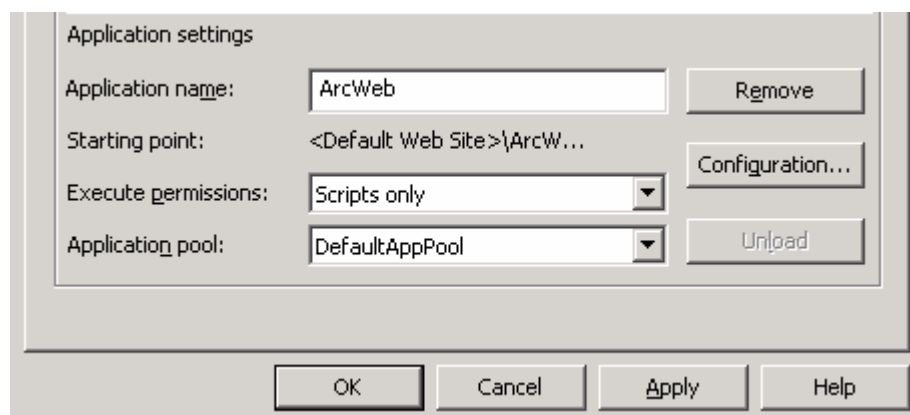


Q: I see the ASP source code when I try to do a report. Or, I get an error 404 when accessing the report (caused by 404.dll being mapped to ASP extensions).



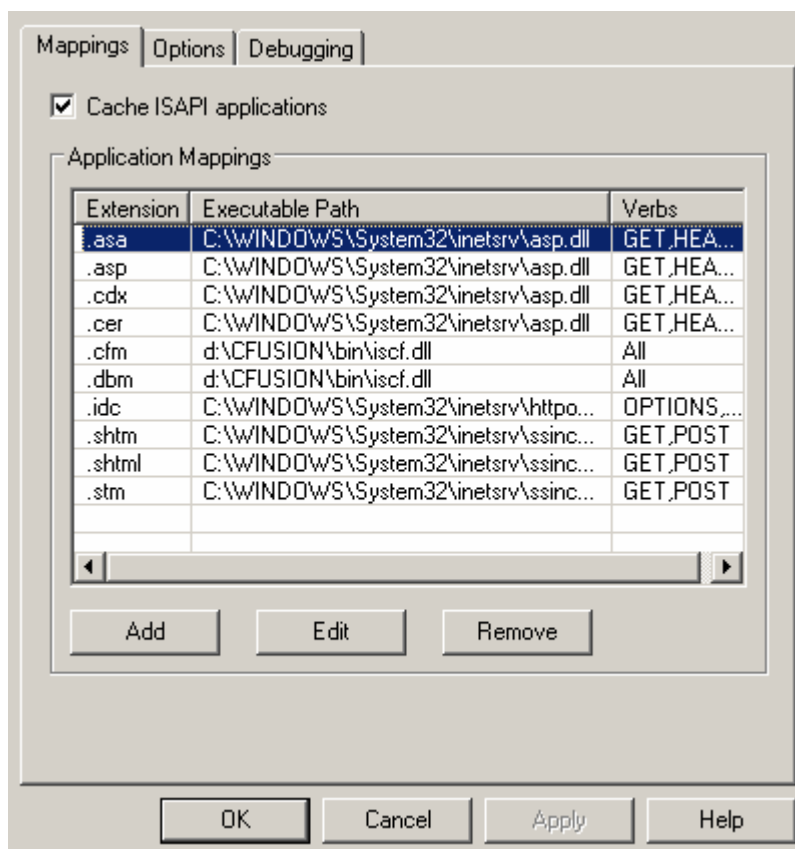
A: The Application Configuration page mapping is missing an entry for ASP.DLL or is pointed to the **404.dll** file. If you are running on a Windows 2003 server, you will need to go to the **Add/Remove Programs** and reconfigure IIS to support ASP pages (disabled by default in Server 2003).

Start the **IIS Configuration** applet. Right click on the web site and select properties. Click on the “**Home Directory**” tab:

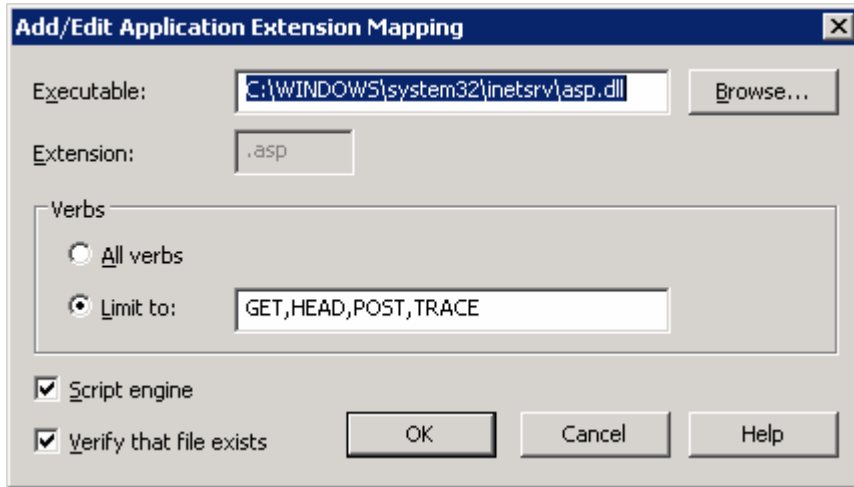


Click on the “**Configuration...**” button located in the lower right area of the page.

You will then see a dialog similar to the following:



Confirm that the entry in the “**Extension**” column for “.asp” points to the asp.dll executable for the verbs “**GET, HEAD, POST, TRACE**” or the single entry of “**ALL**”. If the ASP entry is missing or incorrect, remove the bad entry, click on the “**Add**” button and add the entry as follows:



Please note that the path will be unique for your installation.

Q: When attempting to load the web site, you receive the following error: “**Directory Listing Denied**” or you see the contents of the ArcWeb\www directory.

A: The correct default document has not been defined on the documents tab of your website or virtual directory. Go to the documents tab of the virtual directory or website you setup for ArcWeb and add select “Enable default content page” and add “default.asp” as the default document. Then click OK.

